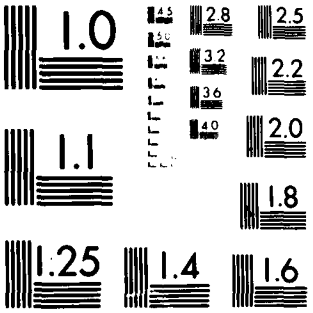
AD-A111 804 STANFORD UNIV CA DEPT OF COMPUTER SCIENCE F/G 9/2
VERIFICATION OF SEQUENTIAL PROGRAMS: TEMPORAL AXIOMATIZATION.(U)
SEP 81 Z MANNA N00014-76-C-0687
UNCLASSIFIED STAN-CS-81-877 NL

1 OF 1
AD
A111804

END
DATE
FILMED
4-82
DTIC



MICROCOPY RESOLUTION TEST CHART

NATIONAL BUREAU OF

September 1981

Report. No. STAN-CS-81-877

(12)

Verification of Sequential Programs: Temporal Axiomatization

by

Zohar Manna

Department of Computer Science

Stanford University
Stanford, CA 94305

VERIFICATION OF SEQUENTIAL PROGRAMS: TEMPORAL AXIOMATIZATION

by

ZOHAR MANNA

Computer Science Dept.
Stanford University
Stanford, CA

Applied Mathematics Dept.
The Weizmann Institute
Rehovot, Israel

Abstract

This is one in a series of reports describing the application of temporal logic to the specification and verification of computer programs.

This report focuses on [illegible] computer

In earlier reports, we introduced temporal logic as a tool for reasoning about concurrent programs *and specifying their properties* [MP1] *and* presented *proof principles for establishing* these properties ([MP2]). ~~Here~~, we restrict ourselves to deterministic, sequential programs. We present a proof system in which properties of such programs, expressed as temporal formulas, can be proved formally.

Our proof system consists of three parts: a *general part* elaborating the properties of temporal logic, a *domain part* giving an axiomatic description of the data domain, and a *program part* giving an axiomatic description of the program under consideration.

is illustrated through the [illegible]

We illustrate the use of the proof system by giving two alternative formal proofs of the total correctness of a simple program.

This paper appears in the *Theoretical Foundations of Programming Methodology* (F. L. Bauer, E. W. Dijkstra, and C. A. R. Hoare, eds.), NATO Scientific Series, D. Reidel Pub. Co., Holland, 1981.

This research was supported in part by the National Science Foundation under grants MCS80-06930, in part by the Office of Naval Research under Contract N00014-76-C-0687, and in part by the United States Air Force Office of Scientific Research under Contract AFOSR-81-0014.

1. INTRODUCTION

Temporal logic is a modal logic in which we impose special restrictions on the models of interpretation ([PRI], [RU],[PNU],[GPSS], [MP1]). A ***universe*** for temporal logic consists of a collection of ***states*** (***worlds***). A state s' is accessible from a state s if through development in time, s can change into s'. We concentrate on histories of development which are linear and discrete. Thus, the models of temporal logic consist of ω-sequences, *i.e.*, infinite sequences of the form $\sigma = s_0, s_1, \ldots$. In such a sequence, s_j is accessible from s_i if $i \leq j$. On these states we define an ***immediate accessibility relation*** ρ which is required to be a function. That means that every state s has exactly one other state s' such that $\rho(s, s')$. This corresponds to our intuition that in a discrete time model each instant has exactly one immediate successor. the transitive reflexive closure of ρ, $R = \rho^*$, is the ***accessibility relation***; intuitively, $R(s, s')$ holds when s' is either identical to s or lies in the future of s.

We first describe the temporal language we are going to use. This language is designed specially for the application we have in mind, namely reasoning about programs, and is not necessarily the most general temporal language possible.

The language uses a set of basic symbols consisting of individual variables and constants, and proposition, function and predicate symbols. The set is partitioned into two subsets: global and local symbols. The ***global symbols*** have a uniform interpretation over the complete universe and do not change their values or meanings from one state to another. The ***local symbols***, on the other hand, may assume different meanings and values in different states of the universe. For our purpose, the only local symbols that interest us are local individual variables. We will have global symbols of all types.

We use the regular set of boolean connectives: $\wedge$, $\vee$, $\supset$, $\equiv$, and $\sim$ together with the equality operator $=$ and the first-order quantifiers $\forall$ and $\exists$. This set is referred to as the ***classical operators***. The quantifiers $\forall$ and $\exists$ are applied only to global individual variables.

The ***modal operators*** used are: $\Box$, $\Diamond$, $\bigcirc$, and $\mathcal{U}$, which are called respectively the ***always***, ***sometime***, ***next*** and ***until*** operators. The first three operators are unary while the $\mathcal{U}$ operator is binary. We use the ***next*** operator $\bigcirc$ in two different ways – as a temporal operator applied to formulas and as a temporal operator applied to terms.

A ***model*** (I, α, σ) for our language consists of a (global) interpretation I, a (global) assignment α and a sequence of states σ.

- The ***interpretation*** I specifies a nonempty domain D and assigns concrete elements, functions and predicates to the (global) individual constants, function [illegible]dicate symbols.

- The ***assignment*** α assigns a value over the appropriate domain to each of the global free individual variables.

- The ***sequence*** $\sigma = s_0, s_1, \ldots$ is an infinite sequence of states. Each ***state*** s_i assigns values to the local free individual variables and propositions.

For a sequence

$$\sigma = s_0, s_1, \ldots$$

we denote by

$$\sigma^{(i)} = s_i, s_{i+1}, \ldots$$

the i-truncated suffix of σ.

Given a temporal formula w, we present below an inductive definition of the truth value of w in a model (I, α, σ). The value of a subformula or term τ under (I, α, σ) is denoted by $\tau|^{\alpha}_{\sigma}$, I being implicitly assumed.

Consider first the evaluation of terms:

- For a local individual variable or local proposition y:

$$y|^{\alpha}_{\sigma} = y_{s_0},$$

i.e., the value assigned to y in s_0, the first state of σ.

- For a global individual variable or global proposition u:

$$u|^{\alpha}_{\sigma} = \alpha[u],$$

i.e., the value assigned to u by α.

- For an individual constant the evaluation is given by I:

$$c|^{\alpha}_{\sigma} = I[c].$$

- For a k-ary function f:

$$f(t_1, \ldots, t_k)|^{\alpha}_{\sigma} = I[f](t_1|^{\alpha}_{\sigma}, \ldots, t_k|^{\alpha}_{\sigma}),$$

i.e., the value is given by the application of the interpreted function $I[f]$ to the values of $t_1, \ldots, t_k$ evaluated in the environment $(I,\ \alpha,\ \sigma)$.

- For a term t:

$$\bigcirc t|^{\alpha}_{\sigma} = t|^{\alpha}_{\sigma^{(1)}},$$

i.e., the value of $\bigcirc t$ in $\sigma = s_0, s_1, \ldots$ is given by the value of t in the shifted sequence $\sigma^{(1)} = s_1, s_2, \ldots$.

Consider now the evaluation of formulas:

- For a k-ary predicate p (including equality):

$$p(t_1, \ldots, t_k)|^{\alpha}_{\sigma} = I[p](t_1|^{\alpha}_{\sigma}, \ldots, t_k|^{\alpha}_{\sigma}).$$

Here again, we evaluate the arguments in the environment and then test $I[p]$ on them.

- For a disjunction:

$$(w_1 \vee w_2)|_{\sigma}^{\alpha} = \textit{true} \quad \textit{iff} \quad w_1|_{\sigma}^{\alpha} = \textit{true} \quad \text{or} \quad w_2|_{\sigma}^{\alpha} = \textit{true}.$$

- For a negation:

$$(\sim w)|_{\sigma}^{\alpha} = \textit{true} \quad \textit{iff} \quad w|_{\sigma}^{\alpha} = \textit{false}.$$

- For a next-time application:

$$\bigcirc w|_{\sigma}^{\alpha} = w|_{\sigma^{(1)}}^{\alpha}.$$

Thus $\bigcirc w$ means: w will be true in the *next* instant – read "next w".

- For an all-times application:

$$\Box w|_{\sigma}^{\alpha} = \textit{true} \quad \textit{iff} \quad \text{for every } k \geq 0,\ w|_{\sigma^{(k)}}^{\alpha} = \textit{true},$$

i.e., w is true for all suffix sequences of σ. Thus $\Box w$ means: w is true for *all* future instants (including the present) – read "always w" or "henceforth w".

- For a some-time application:

$$\Diamond w|_{\sigma}^{\alpha} = \textit{true} \quad \textit{iff} \quad \text{there exists a } k \geq 0 \text{ such that } w|_{\sigma^{(k)}}^{\alpha} = \textit{true},$$

i.e., w is *true* on at least one suffix of σ. Thus $\Diamond w$ means: w will be true for *some* future instant (possibly the present) – read "sometimes w" or "eventually w".

- For an until application:

$$\begin{aligned} w_1 \mathcal{U} w_2|_{\sigma}^{\alpha} = \textit{true} \quad \textit{iff} \quad & \text{for some } k \geq 0,\ w_2|_{\sigma^{(k)}}^{\alpha} = \textit{true} \text{ and} \\ & \text{for all } i,\ 0 \leq i < k,\ w_1|_{\sigma^{(i)}}^{\alpha} = \textit{true}. \end{aligned}$$

Thus $w_1 \mathcal{U} w_2$ means: there is a future instant in which w_2 holds, and such that ***until*** that instant w_1 continuously holds – read "w_1 until w_2"([KAM], [GPSS]).

- For a universal quantification:

$$(\forall u.w)|_{\sigma}^{\alpha} = \textit{true} \quad \textit{iff} \quad \text{for every } d \in D,\ w|_{\sigma}^{\alpha'} = \textit{true},$$

where $\alpha' = \alpha \circ [u \leftarrow d]$ is the assignment obtained from α by assigning d to u.

- For an existential quantification:

$$(\exists u.w)|_{\sigma}^{\alpha} = \textit{true} \quad \textit{iff} \quad \text{for some } d \in D,\ w|_{\sigma}^{\alpha'} = \textit{true},$$

where $\alpha' = \alpha \circ [u \leftarrow d]$.

A formula w is *valid* if it is true in every model (I, α, σ).

Having defined valid formulas, we naturally look for a deductive system. In such a system we take some of the valid formulas as basic axioms and provide a set of sound inference rules by which we hope to be able to prove the other valid formulas as theorems. In order to denote the fact that a formula w is a theorem derivable in our deductive system we will write $\vdash w$. This will be the case if w is an axiom or is derivable from the axioms by a *proof* using the inference rules of the system.

We partition our deductive system into a ***general part*** dealing with the general temporal properties of discrete linear sequences, a ***domain part*** which gives an axiomatic description of the necessary knowledge about the domain, and a ***program part*** which gives an axiomatic description of a particular program.

We start with the general part, describing first the axiomatic system for propositional temporal logic in which we do not admit predicates or quantification. We treat first the "classical" modal operators $\Box$ and $\Diamond$ (the *modal system*), and later add the special operators $\bigcirc$ and $\mathcal{U}$ (the *temporal system*).

2. THE $\Box$ ("ALWAYS") AND $\Diamond$ ("SOMETIME") OPERATORS

Axioms:

$A1.\quad \vdash\ \sim\Diamond w \equiv \Box\sim w$

$A2.\quad \vdash\ \Box(w_1 \supset w_2)\ \supset\ (\Box w_1 \supset \Box w_2)$

$A3.\quad \vdash\ \Box w \supset w$

$A4.\quad \vdash\ \Box w \supset \Box\Box w$

Axiom $A1$ defines $\Diamond$ as the dual of $\Box$; it states that at all times w is false *iff* it is not the case that sometime w holds. Axiom $A2$ states that if universally w_1 implies w_2 then if at all times w_1 is true then so is w_2. Axiom $A3$ establishes the present as part of the future by stating that if w is true at all future times it must be true of the present. Axiom $A4$ states that if w holds in the future, it holds in the future of the future.

Inference rules:

$R1$. If w is an instance of a propositional tautology then $\vdash w$
(*Propositional Tautology* – *PT*)

$R2$. If $\vdash w_1 \supset w_2$ and $\vdash w_1$ then $\vdash w_2$
(*Modus Ponens* – *MP*)

$R3$. If $\vdash w$ then $\vdash \Box w$
($\Box$ *Insertion* – $\Box I$)

All these rules are sound. The soundness of $R1$ and $R2$ is obvious. Note that in $R1$ we also include modal instances of tautologies; we may substitute an arbitrary modal formula for a proposition letter in obtaining an instance. For example $\Box w \supset \Box w$ is a modal instance of the tautology $p \supset p$. To justify $R3$, we recall that validity of w means that w is true in *all* models, hence $\Box w$ is also valid.

This system provides a logical basis for "propositional" modal reasoning. In Modal Logic circles, this system is known as $S4$ (see, *e.g.*, [HC]). This system constrains R to be reflexive ($A3$) and transitive ($A4$).

Before demonstrating some theorems that can be proved in this system, we develop several useful derived rules:

Propositional Reasoning — *PR*

$$\frac{\vdash (w_1 \wedge w_2 \wedge \ldots \wedge w_n) \supset w \qquad \vdash w_1,\ \vdash w_2,\ \ldots,\ \text{and}\ \vdash w_n}{\vdash w}$$

The notation above is used to describe inference rules. It has the general form

$$\frac{\vdash \varphi_1,\ \vdash \varphi_2\ \ldots,\ \vdash \varphi_m}{\vdash \psi}$$

and means that if we have already proved $\varphi_1, \ldots, \varphi_m$ (the ***assumptions*** of the rule), we are allowed by this rule to infer ψ (the ***conclusion*** of the rule).

proof:

The rule follows from the propositional tautology (Rule $R1$)

$$\vdash\ [(w_1 \wedge w_2 \wedge \ldots \wedge w_n) \supset w]\ \supset\ [w_1 \supset (w_2 \supset (\ldots(w_n \supset w)\ldots))]$$

by applying MP (Rule $R2$) $n+1$ times. ∎

Whenever we apply this derived rule without indicating the antecedent

$$\vdash\ (w_1 \wedge w_2 \ldots \wedge w_n) \supset w,$$

it means that this formula is simply an instance of a propositional tautology.

$\Box\Box$ *Rules*

(a) $$\frac{\vdash w_1 \supset w_2}{\vdash \Box w_1 \supset \Box w_2}$$ (b) $$\frac{\vdash w_1 \equiv w_2}{\vdash \Box w_1 \equiv \Box w_2}$$

proof of (a):

1. $\vdash\ w_1 \supset w_2$ given
2. $\vdash\ \Box(w_1 \supset w_2)$ by $\Box I$
3. $\vdash\ \Box(w_1 \supset w_2) \supset (\Box w_1 \supset \Box w_2)$ by $A2$
4. $\vdash\ \Box w_1 \supset \Box w_2$ by 2, 3, and MP

Rule (b) then follows by propositional reasoning, since

$$[(w_1 \supset w_2) \wedge (w_2 \supset w_1)] \equiv (w_1 \equiv w_2)$$

is a tautology. ▮

$\Diamond\Diamond$ *Rules*

(a) $$\frac{\vdash w_1 \supset w_2}{\vdash \Diamond w_1 \supset \Diamond w_2}$$ (b) $$\frac{\vdash w_1 \equiv w_2}{\vdash \Diamond w_1 \equiv \Diamond w_2}$$

proof of (a):

1. $\vdash\ w_1 \supset w_2$ given
2. $\vdash\ \sim w_2 \supset \sim w_1$ by PR
3. $\vdash\ \Box\sim w_2 \supset \Box\sim w_1$ by $\Box\Box$
4. $\vdash\ \sim\Diamond w_2 \supset \sim\Diamond w_1$ by $A1$ and PR
5. $\vdash\ \Diamond w_1 \supset \Diamond w_2$ by PR

Rule (b) then follows by propositional reasoning. ▮

Equivalence Rule – ER

Let w' be the result of replacing an occurrence of a subformula v_1 in w by v_2. Then

$$\frac{\vdash v_1 \equiv v_2}{\vdash w \equiv w'}$$

proof:

By induction on the structure of w.

Case: w is v_1. Then w' is v_2 and $\vdash v_1 \equiv v_2$ implies $\vdash w \equiv w'$.

Case: w is of the form $\sim u$. We assume that $\vdash v_1 \equiv v_2$ implies $\vdash u \equiv u'$. Then by propositional reasoning $\vdash \sim u \equiv \sim u'$, *i.e.*, $\vdash w \equiv w'$.

Case: w is of the form $u_1 \vee u_2$. We assume that if $\vdash v_1 \equiv v_2$, then $\vdash u_1 \equiv u_1'$ and $\vdash u_2 \equiv u_2'$. Then by propositional reasoning $\vdash (u_1 \vee u_2) \equiv (u_1' \vee u_2')$, *i.e.*, $\vdash w \equiv w'$.

The cases where w is of form $u_1 \wedge u_2$, $u_1 \supset u_2$, *etc.* are similar.

Case: w is of the form $\Box u$. We assume that if $\vdash v_1 \equiv v_2$, then $\vdash u \equiv u'$. By the $\Box\Box$-rule, $\vdash \Box u \equiv \Box u'$, *i.e.*, $\vdash w \equiv w'$.

The case in which w is of the form $\Diamond u$ is treated similarly, using the $\Diamond\Diamond$-rule. ∎

Some theorems that can be derived in the system are:

*T*1. $\vdash w \supset \Diamond w$

proof:

1.	$\vdash (\Box \sim w) \supset \sim w$	by *A*3
2.	$\vdash w \supset (\sim \Box \sim w)$	by *PR*
3.	$\vdash w \supset \Diamond w$	by *A*1 and *PR*

The theorem implies (by *MP*)

$\Diamond$ ***Insertion*** - $\Diamond I$

$$\frac{\vdash \ w}{\vdash \ \Diamond w}$$

We can derive the converse of axiom *A*4 as stated in the modal system, and thus prove:

*T*2. $\vdash \Box w \equiv \Box\Box w$

proof:

1.	$\vdash \Box w \supset \Box\Box w$	by *A*4
2.	$\vdash \Box w \supset w$	by *A*3
3.	$\vdash \Box\Box w \supset \Box w$	by $\Box\Box$
4.	$\vdash \Box w \equiv \Box\Box w$	by 1, 3, and *PR*

*T*3. $\vdash \Diamond w \equiv \Diamond\Diamond w$

proof:

1.	$\vdash \Box \sim w \equiv \Box\Box \sim w$	by *T*2

2. $\vdash\ \sim\Box\sim w \ \equiv\ \sim\Box\Box\sim w$ — by *PR*
3. $\vdash\ \Diamond w \ \equiv\ \sim\Box\sim\Diamond w$ — by *A*1 and *ER*
4. $\vdash\ \Diamond w \ \equiv\ \Diamond\Diamond w$ — by *A*1 and *PR*

Because of these last two theorems we can collapse any string of consecutive identical modalities such as $\Box \cdots \Box$ or $\Diamond \cdots \Diamond$ into a single modality of the same type.

Note that to derive line 3 from line 2 we could not use propositional reasoning (*PR*), but we had to use the equivalence rule (*ER*). The subformula $\Box \sim w$ in

2. $\vdash\ \ldots \ \equiv\ \sim\Box\Box\sim w$

was replaced by the equivalent subformula $\sim\Diamond w$ to obtain

3. $\vdash\ \ldots \ \equiv\ \sim\Box\sim\Diamond w.$

But this replacement is inside $\Box$ and thus cannot be justified by propositional reasoning. The replacement done on the left-hand side of the equivalence can be justified by propositional reasoning.

*T*4. $\vdash\ (\Diamond\sim w) \ \equiv\ (\sim\Box w)$

proof:

1. $\vdash\ (\sim\sim w) \ \equiv\ w$ — by *PT*
2. $\vdash\ (\Box\sim\sim w) \ \equiv\ \Box w$ — by $\Box\Box$
3. $\vdash\ (\sim\Diamond\sim w) \ \equiv\ \Box w$ — by *A*1 and *PR*
4. $\vdash\ (\Diamond\sim w) \ \equiv\ (\sim\Box w)$ — by *PR*

*T*5. $\vdash\ \Box(w_1 \supset w_2) \ \supset\ (\Diamond w_1 \supset \Diamond w_2)$

proof:

1. $\vdash\ (w_1 \supset w_2) \ \equiv\ (\sim w_2 \supset \sim w_1)$ — by *PT*
2. $\vdash\ \Box(w_1 \supset w_2) \ \equiv\ \Box(\sim w_2 \supset \sim w_1)$ — by $\Box\Box$
3. $\vdash\ \Box(\sim w_2 \supset \sim w_1) \ \supset\ (\Box\sim w_2 \supset \Box\sim w_1)$ — by *A*2
4. $\vdash\ (\Box\sim w_2 \supset \Box\sim w_1) \ \equiv\ (\sim\Diamond w_2 \supset \sim\Diamond w_1)$ — by *A*1 and *PR*
5. $\vdash\ (\sim\Diamond w_2 \supset \sim\Diamond w_1) \ \equiv\ (\Diamond w_1 \supset \Diamond w_2)$ — by *PT*
6. $\vdash\ \Box(w_1 \supset w_2) \ \supset\ (\Diamond w_1 \supset \Diamond w_2)$ — by 2, 3, 4, 5, and *PR*

*T*6. $\vdash\ \Box(w_1 \wedge w_2) \ \equiv\ (\Box w_1 \wedge \Box w_2)$

proof:

1. $\vdash\ (w_1 \wedge w_2) \ \supset\ w_1$ — by *PT*
2. $\vdash\ \Box(w_1 \wedge w_2) \ \supset\ \Box w_1$ — by $\Box\Box$
3. $\vdash\ (w_1 \wedge w_2) \ \supset\ w_2$ — by *PT*
4. $\vdash\ \Box(w_1 \wedge w_2) \ \supset\ \Box w_2$ — by $\Box\Box$
5. $\vdash\ \Box(w_1 \wedge w_2) \ \supset\ (\Box w_1 \wedge \Box w_2)$ — by 2, 4, and *PR*
6. $\vdash\ w_1 \ \supset\ (w_2 \supset w_1 \wedge w_2)$ — by *PT*

7. $\vdash \ \Box w_1 \ \supset \ \Box(w_2 \supset (w_1 \wedge w_2))$ by $\Box\Box$

8. $\vdash \ \Box(w_2 \supset (w_1 \wedge w_2)) \ \supset \ (\Box w_2 \supset \Box(w_1 \wedge w_2))$ by *A2*

9. $\vdash \ \Box w_1 \ \supset \ (\Box w_2 \supset \Box(w_1 \wedge w_2))$ by 7, 8, and *PR*

10. $\vdash \ (\Box w_1 \wedge \Box w_2) \ \supset \ \Box(w_1 \wedge w_2)$ by *PR*

11. $\vdash \ \Box(w_1 \wedge w_2) \ \equiv \ (\Box w_1 \wedge \Box w_2)$ by 5, 10, and *PR*

T7. $\vdash \ \Diamond(w_1 \vee w_2) \ \equiv \ (\Diamond w_1 \vee \Diamond w_2)$

proof:

1. $\vdash \ \Box(\sim w_1 \wedge \sim w_2) \ \equiv \ (\Box \sim w_1 \wedge \Box \sim w_2)$ by *T6*

2. $\vdash \ \Box \sim (w_1 \vee w_2) \ \equiv \ \sim(\sim \Box \sim w_1 \vee \sim \Box \sim w_2)$ by *ER*

3. $\vdash \ \sim \Diamond(w_1 \vee w_2) \ \equiv \ \sim(\Diamond w_1 \vee \Diamond w_2)$ by *A1* and *PR*

4. $\vdash \ \Diamond(w_1 \vee w_2) \ \equiv \ (\Diamond w_1 \vee \Diamond w_2)$ by *PR*

Note that because of the universal character of $\Box$ it can be distributed over $\wedge$ (Theorem *T6*), while $\Diamond$, which is of existential character can be distributed over $\vee$ (Theorem *T7*).

T8. $\vdash \ \Diamond(w_1 \wedge w_2) \ \supset \ (\Diamond w_1 \wedge \Diamond w_2)$

proof:

1. $\vdash \ \Diamond(w_1 \wedge w_2) \ \supset \ \Diamond w_1$ by *PT* and $\Diamond\Diamond$

2. $\vdash \ \Diamond(w_1 \wedge w_2) \ \supset \ \Diamond w_2$ by *PT* and $\Diamond\Diamond$

3. $\vdash \ \Diamond(w_1 \wedge w_2) \ \supset \ (\Diamond w_1 \wedge \Diamond w_2)$ by 1, 2, and *PR*

T9. $\vdash \ (\Box w_1 \vee \Box w_2) \ \supset \ \Box(w_1 \vee w_2)$

proof:

1. $\vdash \ \Box w_1 \ \supset \ \Box(w_1 \vee w_2)$ by *PT* and $\Box\Box$

2. $\vdash \ \Box w_2 \ \supset \ \Box(w_1 \vee w_2)$ by *PT* and $\Box\Box$

3. $\vdash \ (\Box w_1 \vee \Box w_2) \ \supset \ \Box(w_1 \vee w_2)$ by 1, 2, and *PR*

T10. $\vdash \ (\Box w_1 \wedge \Diamond w_2) \ \supset \ \Diamond(w_1 \wedge w_2)$

proof:

1. $\vdash \ \Box(w_1 \supset \sim w_2) \ \supset \ (\Box w_1 \supset \Box \sim w_2)$ by *A2*

2. $\vdash \ \Box \sim (w_1 \wedge w_2) \ \supset \ \sim(\Box w_1 \wedge \sim \Box \sim w_2)$ by *ER*

3. $\vdash \ \sim \Diamond(w_1 \wedge w_2) \ \supset \ \sim(\Box w_1 \wedge \Diamond w_2)$ by *A1* and *PR*

4. $\vdash \ (\Box w_1 \wedge \Diamond w_2) \ \supset \ \Diamond(w_1 \wedge w_2)$ by *PR*

another proof (without using ER):

1. $\vdash \ w_1 \ \supset \ (w_2 \supset (w_1 \wedge w_2))$ by *PT*

2. $\vdash \ \Box w_1 \ \supset \ \Box(w_2 \supset (w_1 \wedge w_2))$ by $\Box\Box$

3. $\vdash \Box(w_2 \supset (w_1 \wedge w_2)) \supset (\Diamond w_2 \supset \Diamond(w_1 \wedge w_2))$ by $T5$
4. $\vdash \Box w_1 \supset (\Diamond w_2 \supset \Diamond(w_1 \wedge w_2))$ by 2, 3, and PR
5. $\vdash (\Box w_1 \wedge \Diamond w_2) \supset \Diamond(w_1 \wedge w_2)$ by PR

The following derived rules correspond to proof rules existing in most axiomatic verification systems:

Consequence Rules – $\Diamond Q$ *and* $\Box Q$

$$\frac{\begin{array}{l}\vdash w_1 \supset w_2 \\ \vdash w_2 \supset \Diamond w_3 \\ \vdash w_3 \supset w_4\end{array}}{\vdash w_1 \supset \Diamond w_4} \qquad \frac{\begin{array}{l}\vdash w_1 \supset w_2 \\ \vdash w_2 \supset \Box w_3 \\ \vdash w_3 \supset w_4\end{array}}{\vdash w_1 \supset \Box w_4}$$

proof of $\Diamond Q$*:*

1. $\vdash w_1 \supset w_2$ given
2. $\vdash w_2 \supset \Diamond w_3$ given
3. $\vdash w_3 \supset w_4$ given
4. $\vdash \Diamond w_3 \supset \Diamond w_4$ by 3 and $\Diamond\Diamond$
5. $\vdash w_1 \supset \Diamond w_4$ by 1, 2, 4, and PR

The $\Box Q$ rule is proved similarly by the $\Box\Box$-rule.

Concatenation Rule – $\Diamond C$ *and* $\Box C$

$$\frac{\begin{array}{l}\vdash w_1 \supset \Diamond w_2 \\ \vdash w_2 \supset \Diamond w_3\end{array}}{\vdash w_1 \supset \Diamond w_3} \qquad \frac{\begin{array}{l}\vdash w_1 \supset \Box w_2 \\ \vdash w_2 \supset \Box w_3\end{array}}{\vdash w_1 \supset \Box w_3}$$

proof of $\Diamond C$*:*

1. $\vdash w_1 \supset \Diamond w_2$ given
2. $\vdash w_2 \supset \Diamond w_3$ given
3. $\vdash \Diamond w_2 \supset \Diamond\Diamond w_3$ by 2 and $\Diamond\Diamond$
4. $\vdash \Diamond w_2 \supset \Diamond w_3$ by $T3$ and PR
5. $\vdash w_1 \supset \Diamond w_3$ by 1, 4, and PR

The $\Box C$ rule is proved similarly by the $\Box\Box$-rule.

3. THE $\bigcirc$ ("NEXT") AND $\mathcal{U}$ ("UNTIL") OPERATORS

Axioms:

$C1.\quad \vdash\ \sim\Diamond w \equiv \Box\sim w$

$C2.\quad \vdash\ \Box(w_1 \supset w_2) \supset (\Box w_1 \supset \Box w_2)$

$C3.\quad \vdash\ \Box w \supset w$

$C4.\quad \vdash\ \bigcirc\sim w \equiv \sim\bigcirc w$

$C5.\quad \vdash\ \bigcirc(w_1 \supset w_2) \supset (\bigcirc w_1 \supset \bigcirc w_2)$

$C6.\quad \vdash\ \Box w \supset \bigcirc w$

$C7.\quad \vdash\ \Box w \supset \bigcirc\Box w$

$C8.\quad \vdash\ \Box(w \supset \bigcirc w) \supset (w \supset \Box w)$

$C9.\quad \vdash\ w_1\, \mathcal{U}\, w_2 \equiv [w_2 \vee (w_1 \wedge \bigcirc(w_1\, \mathcal{U}\, w_2))]$

$C10.\quad \vdash\ w_1\, \mathcal{U}\, w_2 \supset \Diamond w_2.$

Axioms $C1 - C3$ are the same as $A1 - A3$ in the modal system.

Axiom $C4$ establishes $\bigcirc$ as self-dual. Consequently it implies that the next instant exists and is unique, and restricts our models to linear sequences (no branching).

Axiom $C5$ is the analogue of $C2$ for the $\bigcirc$ operator. Axiom $C6$ states that the next instant is one of the reachable states, *i.e.*, it is also part of the future. Axiom $C7$ is a weaker version of $A4$, $\vdash \Box w \supset \Box\Box w$, and can be used together with $C8$ to prove $A4$ as a theorem in this system. Axiom $C8$ is the "computational induction" axiom; it states that if a property is inherited over one step transitions, it is invariant over any suffix sequence whose first state satisfies w. Axiom $C9$ defines the *until* operator by distributing its effect into what is implied for the present and what is implied for the next instant. Axiom $C10$ simply states that "w_1 until w_2" implies that w_2 will eventually happen.

Inference rules:

*R*1. If w is an instance of a propositional tautology then $\vdash w$
(*Propositional Tautology – PT*)

*R*2. If $\vdash w_1 \supset w_2$ and $\vdash w_1$ then $\vdash w_2$
(*Modus Ponens – MP*)

*R*3. If $\vdash w$ then $\vdash \Box w$
($\Box$ *Insertion* – $\Box I$)

These rules are identical to $R1 - R3$ of the modal system. Since axioms $C1$, $C2$ and $C3$ are identical to axioms $A1$, $A2$ and $A3$ and we will show later that axiom $A4$ is derivable in this system, it follows that all the derived rules of inference and the theorems in the modal system are also derivable in this system. Here are several additional derived rules:

$\bigcirc$ *Insertion* – $\bigcirc I$:

$$\frac{\vdash\ w}{\vdash\ \bigcirc w}$$

proof:

1. $\vdash\ w$ given
2. $\vdash\ \Box w$ by $\Box I$
3. $\vdash\ \bigcirc w$ by $C6$ and MP

$\bigcirc\bigcirc$ *Rules*

$$\text{(a)}\quad \frac{\vdash\ w_1 \supset w_2}{\vdash\ \bigcirc w_1 \supset \bigcirc w_2} \qquad\qquad \text{(b)}\quad \frac{\vdash\ w_1 \equiv w_2}{\vdash\ \bigcirc w_1 \equiv \bigcirc w_2}$$

proof of (a):

1. $\vdash\ w_1 \supset w_2$ given
2. $\vdash\ \bigcirc(w_1 \supset w_2)$ by $\bigcirc I$
3. $\vdash\ \bigcirc w_1 \supset \bigcirc w_2$ by $C5$ and MP

Rule (b) follows by propositional reasoning.

Computational Induction Rule – CI

$$\frac{\vdash\ w \supset \bigcirc w}{\vdash\ w \supset \Box w}$$

proof:

1.	$\vdash\ w \supset \bigcirc w$	given
2.	$\vdash\ \Box(w \supset \bigcirc w)$	by $\Box I$
3.	$\vdash\ \Box(w \supset \bigcirc w) \supset (w \supset \Box w)$	by $C8$
4.	$\vdash\ w \supset \Box w$	by 2, 3, and MP

Backward Induction Rule – BI

$$\frac{\vdash\ \bigcirc w \supset w}{\vdash\ \Diamond w \supset w}$$

proof:

1.	$\vdash\ \bigcirc w \supset w$	given
2.	$\vdash\ \sim w \supset \sim \bigcirc w$	by PR
3.	$\vdash\ \sim w \supset \bigcirc \sim w$	by $C4$ and PR
4.	$\vdash\ \sim w \supset \Box \sim w$	by CI
5.	$\vdash\ \sim w \supset \sim \Diamond w$	by $C1$ and PR
6.	$\vdash\ \Diamond w \supset w$	by PR

$\bigcirc$ *Consequence* Rule – $\bigcirc Q$

$$\frac{\begin{array}{l}\vdash\ w_1 \supset w_2 \\ \vdash\ w_2 \supset \bigcirc w_3 \\ \vdash\ w_3 \supset w_4\end{array}}{\vdash\ w_1 \supset \bigcirc w_4}$$

proof:

1.	$\vdash\ w_1 \supset w_2$	given
2.	$\vdash\ w_2 \supset \bigcirc w_3$	given
3.	$\vdash\ w_3 \supset w_4$	given
4.	$\vdash\ \bigcirc w_3 \supset \bigcirc w_4$	by $\bigcirc\bigcirc$
5.	$\vdash\ w_1 \supset \bigcirc w_4$	by 1, 2, 4, and PR

Note that we do not have a $\bigcirc$ concatenation rule.

A simple theorem of this system is:

$T11.$ $\vdash\ \bigcirc w \supset \Diamond w$

proof:

1.	$\vdash\ (\Box \sim w) \supset (\bigcirc \sim w)$	by $C6$
2.	$\vdash\ (\sim \bigcirc \sim w) \supset (\sim \Box \sim w)$	by PR

3. $\vdash \bigcirc w \supset \Diamond w$ by $C1$, $C4$, and PR

T12. $\vdash \Box w \supset \Box\Box w$

proof:

1. $\vdash \Box w \supset \bigcirc\Box w$ by $C7$
2. $\vdash \Box w \supset \Box\Box w$ by CI

This is the "missing" axiom $A4$. We have all axioms and rules of the previous system, therefore we can deduce all theorems and derived rules of the modal system.

The following special rule is very useful in proving *until* theorems:

Next to Present Rule - NP

$$\begin{array}{l} \vdash (\bigcirc w_1 \equiv \bigcirc w_2) \supset (w_1 \equiv w_2) \\ \vdash w_1 \supset \Diamond(w_1 \land w_2) \\ \vdash w_2 \supset \Diamond(w_1 \land w_2) \\ \hline \vdash w_1 \equiv w_2 \end{array}$$

proof:

1. $\vdash w_1 \supset \Diamond(w_1 \land w_2)$ given
2. $\vdash w_2 \supset \Diamond(w_1 \land w_2)$ given
3. $\vdash (w_1 \lor w_2) \supset \Diamond(w_1 \land w_2)$ by 1, 2, and PR
4. $\vdash (w_1 \land w_2) \supset (w_1 \equiv w_2)$ by PT
5. $\vdash \Diamond(w_1 \land w_2) \supset \Diamond(w_1 \equiv w_2)$ by $\Diamond\Diamond$
6. $\vdash \bigcirc(w_1 \equiv w_2) \supset (w_1 \equiv w_2)$ given
7. $\vdash \Diamond(w_1 \equiv w_2) \supset (w_1 \equiv w_2)$ by BI
8. $\vdash (w_1 \lor w_2) \supset (w_1 \equiv w_2)$ by 3, 5, 7, and PR
9. $\vdash w_1 \equiv w_2$ by PR

We extend now the Equivalence Rule (ER) to handle the $\bigcirc$ and $\mathcal{U}$ operators.

Equivalence Rule - ER

Let w' be the result of replacing an occurrence of a subformula v_1 in w by v_2. Then

$$\begin{array}{c} \vdash v_1 \equiv v_2 \\ \hline \vdash w \equiv w' \end{array}$$

proof:

As before, the proof is by induction on the structure of w. The cases where w is w_1 or of form $\sim u$, $u_1 \vee u_2$, $u_1 \supset u_2$, etc. are treated as in the ER derived rule above.

Case: w is of form $\bigcirc u$. We assume that if $\vdash v_1 \equiv v_2$, then $\vdash u \equiv u'$. Then by the $\bigcirc\bigcirc$-rule $\vdash \bigcirc u \equiv \bigcirc u'$, *i.e.* $\vdash w \equiv w'$.

The cases where w is of form $\Box u$ and $\Diamond u$ are proved similarly by the $\Box\Box$-rule and $\Diamond\Diamond$-rule, respectively. The case that w is of form $u_1 \mathcal{U} u_2$ needs a more detailed proof.

Case: w is of form $u_1 \mathcal{U} u_2$. We assume that if $\vdash v_1 \equiv v_2$, then $\vdash u_1 \equiv u_1'$ and $\vdash u_2 \equiv u_2'$. We attempt to use the Next to Present derived rule (NP) taking w_1 to be $u_1 \mathcal{U} u_2$ and w_2 to be $u_1' \mathcal{U} u_2'$.

1. $\vdash u_1 \equiv u_1'$ induction hypothesis
2. $\vdash u_2 \equiv u_2'$ induction hypothesis
3. $\vdash u_1 \mathcal{U} u_2 \equiv [u_2 \vee (u_1 \wedge \bigcirc(u_1 \mathcal{U} u_2)])$ by $C9$
4. $\vdash u_1' \mathcal{U} u_2' \equiv [u_2' \vee (u_1' \wedge \bigcirc(u_1' \mathcal{U} u_2'))]$ by $C9$
5. $\vdash u_1' \mathcal{U} u_2' \equiv [u_2 \vee (u_1 \wedge \bigcirc(u_1' \mathcal{U} u_2'))]$ by 1, 2, 4, and PR
6. $\vdash [\bigcirc(u_1 \mathcal{U} u_2) \equiv \bigcirc(u_1' \mathcal{U} u_2')] \supset [(u_1 \mathcal{U} u_2) \equiv (u_1' \mathcal{U} u_2')]$ by 3, 5, and PR

7. $\vdash u_1 \mathcal{U} u_2 \supset \Diamond u_2$ by $C10$
8. $\vdash u_2 \supset [(u_1 \mathcal{U} u_2) \wedge (u_1' \mathcal{U} u_2')]$ by 3, 5, and PR
9. $\vdash u_1 \mathcal{U} u_2 \supset \Diamond[(u_1 \mathcal{U} u_2) \wedge (u_1' \mathcal{U} u_2')]$ by 7, 8, and $\Diamond Q$

10. $\vdash u_1' \mathcal{U} u_2' \supset \Diamond u_2'$ by $C10$
11. $\vdash \Diamond u_2 \equiv \Diamond u_2'$ by 2 and $\Diamond\Diamond$
12. $\vdash u_1' \mathcal{U} u_2' \supset \Diamond u_2$ by 10, 11, and PR
13. $\vdash u_1' \mathcal{U} u_2' \supset \Diamond[(u_1 \mathcal{U} u_2) \wedge (u_1' \mathcal{U} u_2')]$ by 8, 12, and $\Diamond Q$

14. $\vdash (u_1 \mathcal{U} u_2) \equiv (u_1' \mathcal{U} u_2')$ by 6, 9, 13, and NP

This concludes the proof. ▮

"next" theorems

T13. $\vdash \bigcirc(w_1 \wedge w_2) \equiv (\bigcirc w_1 \wedge \bigcirc w_2)$

proof:

1. $\vdash \bigcirc(w_1 \supset \sim w_2) \supset (\bigcirc w_1 \supset \bigcirc \sim w_2)$ by $C5$
2. $\vdash \sim(\bigcirc w_1 \supset \bigcirc \sim w_2) \supset \sim \bigcirc(w_1 \supset \sim w_2)$ by PR
3. $\vdash \sim(\bigcirc w_1 \supset \sim \bigcirc w_2) \supset \bigcirc \sim(w_1 \supset \sim w_2)$ by $C4$ and PR
4. $\vdash (\bigcirc w_1 \wedge \bigcirc w_2) \supset \bigcirc(w_1 \wedge w_2)$ by ER

5. $\vdash (w_1 \wedge w_2) \supset w_1$ by PT

6. $\vdash \bigcirc(w_1 \wedge w_2) \supset \bigcirc w_1$ — by $\bigcirc\bigcirc$
7. $\vdash (w_1 \wedge w_2) \supset w_2$ — by *PT*
8. $\vdash \bigcirc(w_1 \wedge w_2) \supset \bigcirc w_2$ — by $\bigcirc\bigcirc$
9. $\vdash \bigcirc(w_1 \wedge w_2) \supset (\bigcirc w_1 \wedge \bigcirc w_2)$ — by 6, 8, and *PR*

10. $\vdash \bigcirc(w_1 \wedge w_2) \equiv (\bigcirc w_1 \wedge \bigcirc w_2)$ — by 4, 9, and *PR*

*T*14. $\vdash \bigcirc(w_1 \vee w_2) \equiv (\bigcirc w_1 \vee \bigcirc w_2)$

proof:

1. $\vdash \bigcirc(\sim w_1 \wedge \sim w_2) \equiv (\bigcirc \sim w_1) \wedge (\bigcirc \sim w_2)$ — by *T*13
2. $\vdash \bigcirc(\sim w_1 \wedge \sim w_2) \equiv (\sim \bigcirc w_1) \wedge (\sim \bigcirc w_2)$ — by *C*4 and *PR*
3. $\vdash \bigcirc \sim(w_1 \vee w_2) \equiv (\sim \bigcirc w_1) \wedge (\sim \bigcirc w_2)$ — by *ER* and *PR*
4. $\vdash \sim \bigcirc(w_1 \vee w_2) \equiv \sim(\bigcirc w_1 \vee \bigcirc w_2)$ — by *C*4 and *PR*
5. $\vdash \bigcirc(w_1 \vee w_2) \equiv (\bigcirc w_1 \vee \bigcirc w_2)$ — by *PR*

*T*15. $\vdash \bigcirc(w_1 \supset w_2) \equiv (\bigcirc w_1 \supset \bigcirc w_2)$

proof:

1. $\vdash \bigcirc(\sim w_1 \vee w_2) \equiv (\bigcirc \sim w_1) \vee (\bigcirc w_2)$ — by *T*14
2. $\vdash \bigcirc(\sim w_1 \vee w_2) \equiv (\sim \bigcirc w_1) \vee (\bigcirc w_2)$ — by *C*4 and *PR*
3. $\vdash \bigcirc(w_1 \supset w_2) \equiv (\bigcirc w_1 \supset \bigcirc w_2)$ — by *ER* and *PR*

*T*16. $\vdash \bigcirc(w_1 \equiv w_2) \equiv (\bigcirc w_1 \equiv \bigcirc w_2)$

proof:

1. $\vdash [\bigcirc(w_1 \supset w_2) \wedge \bigcirc(w_2 \supset w_1)] \equiv [(\bigcirc w_1 \supset \bigcirc w_2) \wedge (\bigcirc w_2 \supset \bigcirc w_1)]$ — by *T*15 and *PR*

2. $\vdash \bigcirc[(w_1 \supset w_2) \wedge (w_2 \supset w_1)] \equiv [(\bigcirc w_1 \supset \bigcirc w_2) \wedge (\bigcirc w_2 \supset \bigcirc w_1)]$ — by *T*13 and *PR*

3. $\vdash \bigcirc(w_1 \equiv w_2) \equiv (\bigcirc w_1 \equiv \bigcirc w_2)$ — by *ER* and *PR*

*T*17. $\vdash \bigcirc\Box w \equiv \Box\bigcirc w$

proof:

1. $\vdash \bigcirc w \supset (w \supset \bigcirc w)$ — by *PT*
2. $\vdash \Box\bigcirc w \supset \Box(w \supset \bigcirc w)$ — by $\Box\Box$
3. $\vdash \Box(w \supset \bigcirc w) \supset \bigcirc\Box(w \supset \bigcirc w)$ — by *C*7
4. $\vdash \bigcirc\Box(w \supset \bigcirc w) \supset \bigcirc(w \supset \Box w)$ — by *C*8 and $\bigcirc\bigcirc$
5. $\vdash \bigcirc(w \supset \Box w) \supset (\bigcirc w \supset \bigcirc\Box w)$ — by *C*5
6. $\vdash \Box\bigcirc w \supset (\bigcirc w \supset \bigcirc\Box w)$ — by 2, 3, 4, 5, and *PR*
7. $\vdash \Box\bigcirc w \supset \bigcirc w$ — by *C*3
8. $\vdash \Box\bigcirc w \supset \bigcirc\Box w$ — by 6, 7, and *PR*

9. $\vdash \bigcirc\Box w \supset \bigcirc\bigcirc\Box w$ — by $C7$ and $\bigcirc\bigcirc$

10. $\vdash \bigcirc\Box w \supset \Box\bigcirc\Box w$ — by CI

11. $\vdash \bigcirc\Box w \supset \bigcirc w$ — by $C3$ and $\bigcirc\bigcirc$

12. $\vdash \Box\bigcirc\Box w \supset \Box\bigcirc w$ — by $\Box\Box$

13. $\vdash \bigcirc\Box w \supset \Box\bigcirc w$ — by 10, 12, and PR

14. $\vdash \bigcirc\Box w \equiv \Box\bigcirc w$ — by 8, 13, and PR

*T*18. $\vdash \bigcirc\Diamond w \equiv \Diamond\bigcirc w$

proof:

1. $\vdash \bigcirc\Box\sim w \equiv \Box\bigcirc\sim w$ — by $T17$

2. $\vdash \sim\bigcirc\Diamond w \equiv \sim\Diamond\bigcirc w$ — by $C1$, $C4$, and ER

3. $\vdash \bigcirc\Diamond w \equiv \Diamond\bigcirc w$ — by PR

*T*19. $\vdash \Box w \equiv (w \wedge \bigcirc\Box w)$

proof:

1. $\vdash \Box w \supset w$ — by $C3$

2. $\vdash \Box w \supset \bigcirc\Box w$ — by $C7$

3. $\vdash \Box w \supset (w \wedge \bigcirc\Box w)$ — by 1, 2, and PR

4. $\vdash \bigcirc\Box w \supset \bigcirc(w \wedge \bigcirc\Box w)$ — by $\bigcirc\bigcirc$

5. $\vdash (w \wedge \bigcirc\Box w) \supset \bigcirc(w \wedge \bigcirc\Box w)$ — by PR

6. $\vdash (w \wedge \bigcirc\Box w) \supset \Box(w \wedge \bigcirc\Box w)$ — by CI

7. $\vdash \Box(w \wedge \bigcirc\Box w) \supset (\Box w \wedge \Box\bigcirc\Box w)$ — by $T6$

8. $\vdash \Box(w \wedge \bigcirc\Box w) \supset \Box w$ — by PR

9. $\vdash (w \wedge \bigcirc\Box w) \supset \Box w$ — by 6, 8, and PR

10. $\vdash \Box w \equiv (w \wedge \bigcirc\Box w)$ — by 3, 9, and PR

*T*20. $\vdash \Diamond w \equiv (w \vee \bigcirc\Diamond w)$

proof:

1. $\vdash \Box\sim w \equiv (\sim w \wedge \bigcirc\Box\sim w)$ — by $T19$

2. $\vdash \sim\Diamond w \equiv \sim(w \vee \sim\bigcirc\Box\sim w)$ — by $C1$ and PR

3. $\vdash \sim\Diamond w \equiv \sim(w \vee \bigcirc\Diamond w)$ — by $C4$, $C1$, and ER

4. $\vdash \Diamond w \equiv (w \vee \bigcirc\Diamond w)$ — by PR

*T*21. $\vdash (w \wedge \Diamond\sim w) \supset \Diamond(w \wedge \bigcirc\sim w)$.

This is the dual of the "computational induction" axiom $C8$. It states that if w is true now and is false in the future, then there exists some instant such that w is true at that instant and false at the next.

proof:

1. $\vdash \Box(w \supset \bigcirc w) \supset (w \supset \Box w)$ — by $C8$

2. $\vdash\ \sim(w \supset \Box w) \supset \sim\Box(w \supset \bigcirc w)$ by *PR*

3. $\vdash\ (w \wedge \sim\Box w) \supset \Diamond(w \wedge \sim\bigcirc w)$ by *T4* and *ER*

4. $\vdash\ (w \wedge \Diamond\sim w) \supset \Diamond(w \wedge \bigcirc\sim w)$ by *T4*, *C4*, and *ER*

"until" theorems

T22. $\vdash\ (\bigcirc w_1)\mathcal{U}(\bigcirc w_2) \equiv \bigcirc(w_1 \mathcal{U} w_2)$

Denoting

$w_1^* :\ (\bigcirc w_1)\mathcal{U}(\bigcirc w_2)$

$w_2^* :\ \bigcirc(w_1 \mathcal{U} w_2)$

we have to show $\vdash\ w_1^* \equiv w_2^*$. We will use the Next to Present derived rule (*NP*).

proof:

1. $\vdash\ w_1^* \equiv \bigcirc w_2 \vee (\bigcirc w_1 \wedge \bigcirc w_1^*)$ by *C9*

2. $\vdash\ \bigcirc(w_1 \mathcal{U} w_2) \equiv \bigcirc(w_2 \vee (w_1 \wedge \bigcirc(w_1 \mathcal{U} w_2)))$ by *C9* and $\bigcirc\bigcirc$

3. $\vdash\ w_2^* \equiv \bigcirc w_2 \vee (\bigcirc w_1 \wedge \bigcirc w_2^*)$ by 2, *T13*, *T14*, and *PR*

4. $\vdash\ (\bigcirc w_1^* \equiv \bigcirc w_2^*) \supset (w_1^* \equiv w_2^*)$ by 1, 3 and *PR*

5. $\vdash\ \bigcirc w_2 \supset (w_1^* \wedge w_2^*)$ by 1, 3 and *PR*

6. $\vdash\ \Diamond\bigcirc w_2 \supset \Diamond(w_1^* \wedge w_2^*)$ by $\Diamond\Diamond$

7. $\vdash\ (\bigcirc w_1 \mathcal{U} \bigcirc w_2) \supset \Diamond\bigcirc w_2$ by *C10*

8. $\vdash\ w_1^* \supset \Diamond(w_1^* \wedge w_2^*)$ by 6, 7 and *PR*

9. $\vdash\ w_1 \mathcal{U} w_2 \supset \Diamond w_2$ by *C10*

10. $\vdash\ \bigcirc(w_1 \mathcal{U} w_2) \supset \Diamond\bigcirc w_2$ by 9, $\bigcirc\bigcirc$, and *T18*

11. $\vdash\ w_2^* \supset \Diamond(w_1^* \wedge w_2^*)$ by 6, 10, and *PR*

12. $\vdash\ w_1^* \equiv w_2^*$ by 4, 8, 11 and *NP*

T23. $\vdash\ (w_1 \wedge w_2)\mathcal{U} w_3 \equiv [(w_1 \mathcal{U} w_2) \wedge (w_2 \mathcal{U} w_3)]$

Denoting

$w_1^* :\ (w_1 \wedge w_2)\mathcal{U} w_3$

$w_2^* :\ (w_1 \mathcal{U} w_3) \wedge (w_2 \mathcal{U} w_3)$

we have to show $\vdash\ w_1^* \equiv w_2^*$. We will again use the derived rule NP.

proof:

1. $\vdash\ w_1^* \equiv w_3 \lor ((w_1 \land w_2) \land \bigcirc w_1^*)$ by $C9$
2. $\vdash\ w_1 \mathcal{U} w_3 \equiv w_3 \lor (w_1 \land \bigcirc(w_1 \mathcal{U} w_3))$ by $C9$
3. $\vdash\ w_2 \mathcal{U} w_3 \equiv w_3 \lor (w_2 \land \bigcirc(w_2 \mathcal{U} w_3))$ by $C9$
4. $\vdash\ (w_1 \mathcal{U} w_3) \land (w_2 \mathcal{U} w_3) \equiv w_3 \lor ((w_1 \land w_2) \land \bigcirc(w_1 \mathcal{U} w_3) \land \bigcirc(w_2 \mathcal{U} w_3))$ by 2, 3, and PR
5. $\vdash\ w_2^* \equiv w_3 \lor ((w_1 \land w_2) \land \bigcirc w_2^*)$ by 4, $T13$, and PR
6. $\vdash\ (\bigcirc w_1^* \equiv \bigcirc w_2^*) \supset (w_1^* \equiv w_2^*)$ by 1, 5, and PR
7. $\vdash\ w_3 \supset (w_1^* \land w_2^*)$ by 1, 5, and PR
8. $\vdash\ \Diamond w_3 \supset \Diamond(w_1^* \land w_2^*)$ by $\Diamond\Diamond$
9. $\vdash\ (w_1 \land w_2)\mathcal{U} w_3 \supset \Diamond w_3$ by $C10$
10. $\vdash\ w_1^* \supset \Diamond(w_1^* \land w_2^*)$ by 7, 9, and PR
11. $\vdash\ w_1 \mathcal{U} w_3 \supset \Diamond w_3$ by $C10$
12. $\vdash\ (w_1 \mathcal{U} w_3) \land (w_2 \mathcal{U} w_3) \supset \Diamond w_3$ by PR
13. $\vdash\ w_2^* \supset \Diamond(w_1^* \land w_2^*)$ by 8, 12, and PR
14. $\vdash\ w_1^* \equiv w_2^*$ by 6, 10, 13, and NP

4. QUANTIFIERS

Since we intend to use terms and predicates in our reasoning we have to extend our system to admit individual variables, terms and quantification. Let us consider additional axioms involving quantifiers and their interaction with modalities.

Axioms:

D1. $\vdash\ \sim\exists x.w \equiv \forall x. \sim w$

D2. $\vdash\ (\forall x.w(x)) \supset w(t)$
where t is any term globally free for x in w

D3. $\vdash\ (\forall x. \Box w) \supset (\Box \forall x.w)$

D4. $\vdash\ (\forall x. \bigcirc w) \supset (\bigcirc \forall x.w)$

In these axioms x is any global individual variable. Axioms $D1$ and $D2$ are the usual predicate calculus axioms: $D1$ defines $\exists$ as the dual of $\forall$ and $D2$ is the *instantiation axiom.* Axiom $D3$ is known as the Barcan formula connecting the two universal operators $\forall$ and $\Box$. Axiom $D4$ is the Barcan formula for the $\bigcirc$ operator. The axioms state that since both operators have universal characteristics they commute.

A term t is said to be ***globally free for*** x in w if substitution of t for all free occurrences of x in w: (a) does not create new bound occurrences of (global) variables, and (b) does not create new occurrences of local variables in the scope of a modal operator. A trivial case: if t is x itself, then t is free for x. Condition (b) in this definition is essential. For, otherwise, we could derive the formula

$$(\forall x.\, \Diamond(x < y)) \supset \Diamond(y < y),$$

which is not valid for a local variable y.

An additional rule of inference is:

Inference rule:

R4. $\forall$ *Insertion* – $\forall I$

$$\frac{\vdash w_1 \supset w_2}{\vdash w_1 \supset \forall x.w_2}$$

where x is not free in w_1.

We have the derived rule

Instantiation Rule – *INST*

$$\frac{\vdash w(x)}{\vdash w(t)}$$

where t is any term globally free for x in w.

proof:

1.	$\vdash w(x)$	given
2.	$\vdash \forall x.w(x)$	by $\forall I$ (taking w_1 to be *true*)
3.	$\vdash (\forall x.w(x)) \supset w(t)$	by $D2$
4.	$\vdash w(t)$	by 2, 3, and MP

The following are the duals of $D2$ and $R4$ for the existential quantifier $\exists$:

T24. $\vdash\ w(t) \supset \exists x.w(x)$

where t is any term globally free for x in w.

proof:

1. $\vdash\ (\forall x. \sim w(x)) \supset \ \sim w(t)$ by $D2$
2. $\vdash\ (\sim\exists x.w(x)) \supset \ \sim w(t)$ by $D1$ and PR
3. $\vdash\ w(t) \supset \exists x.w(x)$ by PR

Note that we need here again the additional condition (b) that the substitution of t for x in w does not create new occurrences of local variables in the scope of a modal operator. For otherwise, we could deduce from $T24$

$$\Box(y \leq y) \supset \exists u. \Box(y \leq u),$$

which is not valid for a local variable y.

$\exists$ *Insertion* – $\exists I$

$$\frac{\vdash w_1 \supset w_2}{\vdash \exists x.w_1 \supset w_2}$$

where x is not free in w_2.

proof:

1. $\vdash\ w_1 \supset w_2$ given
2. $\vdash\ \sim w_2 \supset \ \sim w_1$ by PR
3. $\vdash\ \sim w_2 \supset \forall x. \sim w_1$ by $\forall I$ $(R4)$
4. $\vdash\ \sim w_2 \supset \ \sim\exists x.w_1$ by $D1$ and PR
5. $\vdash\ \exists x.w_1 \supset w_2$ by PR

$\forall\forall$ *Rules*

$$\text{(a)}\quad \frac{\vdash w_1 \supset w_2}{\vdash \forall x.w_1 \supset \forall x.w_2} \qquad\qquad \text{(b)}\quad \frac{\vdash w_1 \equiv w_2}{\vdash \forall x.w_1 \equiv \forall x.w_2}$$

proof of (a):

1. $\vdash\ \forall x.w_1 \supset w_1$ by $D2$
2. $\vdash\ w_1 \supset w_2$ given
3. $\vdash\ \forall x.w_1 \supset w_2$ by PR
4. $\vdash\ \forall x.w_1 \supset \forall x.w_2$ by $\forall I$

Rule (b) then follows by propositional reasoning.

∃∃ Rules :

(a) $$\frac{\vdash w_1 \supset w_2}{\vdash \exists x.w_1 \supset \exists x.w_2}$$ (b) $$\frac{\vdash w_1 \equiv w_2}{\vdash \exists x.w_1 \equiv \exists x.w_2}$$

proof of (a):

1.	$\vdash \; w_1 \supset w_2$	given
2.	$\vdash \; (\sim w_2) \supset (\sim w_1)$	by *PR*
3.	$\vdash \; (\forall x. \sim w_2) \supset (\forall x. \sim w_1)$	by ∀∀
4.	$\vdash \; (\sim \exists x.w_2) \supset (\sim \exists x.w_1)$	by *D*1 and *PR*
5.	$\vdash \; \exists x.w_1 \supset \exists x.w_2$	by *PR*

Rule (b) then follows by propositional reasoning.

The last two rules are, of course, classical rules of the predicate calculus, and are brought here only for the sake of completeness and later reference.

We extend now the Equivalence Rule (*ER*), given above for propositional formulas, to handle predicate formulas as well.

Equivalence Rule - ER

Let w' be the result of replacing an occurrence of a subformula v_1 in w by v_2. Then

$$\frac{\vdash v_1 \equiv v_2}{\vdash w \equiv w'}$$

proof:

The proof is by induction on the structure of w. The cases where w is w_1 or of form $\sim u$, $u_1 \vee u_2$, $u_1 \supset u_2$, $\Box u$, $\Diamond u$, $\bigcirc u$ and $u_1 \mathcal{U} u_2$, are treated as before.

Case: w is of form $\forall x.u$. We assume that if $\vdash v_1 \equiv v_2$, then $\vdash u \equiv u'$ Then by the ∀∀-rule $\vdash \forall x.u \equiv \forall x.u'$, *i.e.* $\vdash w \equiv w'$.

The case where w is of form $\exists x.u$, is proved similarly by the ∃∃-rule. ∎

Deduction Rule - DED

$$\frac{w_1 \vdash w_2}{\vdash (\Box w_1) \supset w_2}$$

where the ∀*I* rule (Rule *R*4) is never applied to a free variable of w_1 in the derivation of $w_1 \vdash w_2$.

That is, if under the assumption w_1 we can derive $\vdash w_2$, where rule $R4$ is never applied to a free variable of w_1, then there exists a proof establishing $\vdash (\Box w_1) \supset w_2$. We clearly must also be careful in using any theorem or derived rule such that the $\forall I$ rule was used in its proof.

The additional $\Box$ operator in the conclusion is obviously necessary since in general $w_1 \vdash w_2$ does not imply $\vdash w_1 \supset w_2$. For example, obviously $w \vdash \Box w$ is true (an immediate application of Rule $R3$: $\vdash w$ by assumption and therefore $\vdash \Box w$ by $\Box I$); but $\vdash w \supset \Box w$ is false.

proof:

The proof of the modal Deduction Rule follows the same arguments used in the proof of the classical Deduction Rule of Predicate Calculus. We replace each line $\vdash u_i$ in the proof of $w_1 \vdash w_2$ by the line $\vdash \Box w_1 \supset u_i$, and show that this transformation preserves soundness. That is

given	show
$\vdash u_1$	$\vdash (\Box w_1) \supset u_1$
$\vdash u_2$	$\vdash (\Box w_1) \supset u_2$
$\vdots$	$\vdots$
$\vdash u_i$	$\vdash (\Box w_1) \supset u_i$
$\vdots$	$\vdots$
$\vdash u_m$	$\vdash (\Box w_1) \supset u_m$
i.e. $\vdash w_2$	*i.e.* $\vdash (\Box w_1) \supset w_2$

where u_i is either the assumption w_1, an axiom, or derived from previous u_j's by some rule of inference.

The proof is by a complete induction on i. We assume that for all $k < i$, $\vdash (\Box w_1) \supset u_k$, and prove that $\vdash (\Box w_1) \supset u_i$.

Case: u_i is an axiom.

1. $\vdash u_i$ axiom
2. $\vdash (\Box w_1) \supset u_i$ by PR

Note that $\vdash w'$ implies $\vdash w \supset w'$ for any w, by propositional reasoning.

Case: u_i is w_1.

1. $\vdash (\Box w_1) \supset w_1$ by $C3$

Case: u_i is obtained by Rule $R1$, *i.e.*, u_i is an instance of a tautology.

1. $\vdash u_i$ by PT
2. $\vdash (\Box w_1) \supset u_i$ by PR

Case: u_i is obtained by Rule $R2$ (using previous $\vdash u_k$ and $\vdash u_k \supset u_i$).

1. $\vdash (\Box w_1) \supset u_k$ induction hypothesis

2.	$\vdash (\Box w_1) \supset (u_k \supset u_i)$	induction hypothesis
3.	$\vdash (\Box w_1) \supset u_i$	by 1, 2, and *PR*

Case: u_i is obtained by Rule *R*3 (using previous $\vdash u_k$), *i.e.*, u_i is $\Box u_k$.

1.	$\vdash (\Box w_1) \supset u_k$	induction hypothesis
2.	$\vdash (\Box \Box w_1) \supset \Box u_k$	by $\Box\Box$
3.	$\vdash (\Box w_1) \supset (\Box \Box w_1)$	by *T*12
4.	$\vdash (\Box w_1) \supset \Box u_k$	by 2, 3, and *PR*

Case: u_i is obtained by Rule *R*4 (using previous $\vdash u \supset v$, *i.e.* u_k, to get $\vdash u \supset \forall x.v$, *i.e.* u_i, where x is not free in u).

By our deduction rule assumption, we know also that x is not free in w_1.

1.	$\vdash (\Box w_1) \supset (u \supset v)$	induction hypothesis
2.	$\vdash ((\Box w_1) \land u) \supset v$	by *PR*
3.	$\vdash ((\Box w_1) \land u) \supset \forall x.v$	by *R*4
		(since x is not free in u or w_1)
4.	$\vdash (\Box w_1) \supset (u \supset \forall x.v)$	by *PR* ▮

A different approach to coping with the application of □ insertion rule (Rule *R*3) is to forbid it altogether. We then get the following restricted deduction rule:

Restricted Deduction Rule — RDED

$$\frac{w_1 \vdash w_2}{\vdash w_1 \supset w_2}$$

Provided $\Box I$ (Rule *R*3) is never applied and $\forall I$ (Rule *R*4) is never applied to a free variable of w_1 in the derivation of $w_1 \vdash w_2$.

Here, we are not allowed to use rule $\Box I$ or any theorem or derived rule that $\Box I$ was used in its proof.

The proof of *RDED* follows exactly that of *DED* except that the case in which Rule *R*3 is applied does not arise.

Predicate Theorems

*T*25. $\vdash (\sim\forall x.w) \equiv (\exists x. \sim w)$

proof:

1.	$\vdash (\sim\sim w) \equiv w$	by *PT*
2.	$\vdash (\forall x. \sim\sim w) \equiv \forall x.w$	by ∀∀

3. $\vdash (\sim\exists x. \sim w) \equiv \forall x.w$ by *D*1 and *PR*

4. $\vdash \sim\forall x.w \equiv \exists x. \sim w$ by *PR*

*T*26. $\vdash \forall x.(w_1 \wedge w_2) \equiv (\forall x.w_1 \wedge \forall x.w_2)$

proof:

1. $\vdash \forall x.w_1 \supset w_1$ by *D*2
2. $\vdash \forall x.w_2 \supset w_2$ by *D*2
3. $\vdash (\forall x.w_1 \wedge \forall x.w_2) \supset (w_1 \wedge w_2)$ by 1, 2, and *PR*
4. $\vdash (\forall x.w_1 \wedge \forall x.w_2) \supset \forall x.(w_1 \wedge w_2)$ by $\forall I$

5. $\vdash (w_1 \wedge w_2) \supset w_1$ by *PT*
6. $\vdash \forall x.(w_1 \wedge w_2) \supset \forall x.w_1$ by $\forall\forall$
7. $\vdash (w_1 \wedge w_2) \supset w_2$ by *PT*
8. $\vdash \forall x.(w_1 \wedge w_2) \supset \forall x.w_2$ by $\forall\forall$
9. $\vdash \forall x.(w_1 \wedge w_2) \supset (\forall x.w_1 \wedge \forall x.w_2)$ by 6, 8, and *PR*

10. $\vdash \forall x.(w_1 \wedge w_2) \equiv (\forall x.w_1 \wedge \forall x.w_2)$ by 4, 9, and *PR*

*T*27. $\vdash \exists x.(w_1 \vee w_2) \equiv (\exists x.w_1 \vee \exists x.w_2)$

proof:

1. $\vdash \forall x.(\sim w_1 \wedge \sim w_2) \equiv (\forall x. \sim w_1 \wedge \forall x. \sim w_2)$ by *T*26
2. $\vdash \forall x. \sim (w_1 \vee w_2) \equiv (\forall x. \sim w_1 \wedge \forall x. \sim w_2)$ by *ER*
3. $\vdash \sim\exists x.(w_1 \vee w_2) \equiv (\sim\exists x.w_1 \wedge \sim\exists x.w_2)$ by *D*1 and *PR*
4. $\vdash \exists x.(w_1 \vee w_2) \equiv (\exists x.w_1 \vee \exists x.w_2)$ by *PR*

*T*28. $\vdash (\forall x.\Box w) \equiv (\Box\forall x.w)$

proof:

1. $\vdash (\forall x.w) \supset w$ by *D*2
2. $\vdash (\Box\forall x.w) \supset \Box w$ by $\Box\Box$
3. $\vdash (\Box\forall x.w) \supset (\forall x.\Box w)$ by $\forall I$
4. $\vdash (\forall x.\Box w) \supset (\Box\forall x.w)$ by *D*3
5. $\vdash (\forall x.\Box w) \equiv (\Box\forall x.w)$ by 3, 4, and *PR*

alternative proof of $\vdash (\Box\forall x.w) \supset (\forall x.\Box w)$

1. $\vdash \forall x.w$ assumption
2. $\vdash w$ by *D*2 and *MP*
3. $\vdash \Box w$ by $\Box I$
4. $\vdash \forall x.\Box w$ by $\forall I$

Thus, $\forall x.w \vdash \forall x.\Box w$ and by the deduction rule

5. $\vdash (\Box\forall x.w) \supset (\forall x.\Box w)$

*T*29. $\vdash (\exists x.\Diamond w) \equiv (\Diamond \exists x.w)$

proof:

1.	$\vdash (\forall x.\Box\sim w) \equiv (\Box\forall x.\sim w)$	by *T*28
2.	$\vdash (\forall x.\sim\Diamond w) \equiv (\Box\sim\exists x.w)$	by *C*1, *D*1, and *ER* (twice)
3.	$\vdash (\sim\exists x.\Diamond w) \equiv (\sim\Diamond\exists x.w)$	by *C*1, *D*1 and *PR*
4.	$\vdash (\exists x.\Diamond w) \equiv (\Diamond\exists x.w)$	by *PR*

*T*30. $\vdash (\bigcirc\forall x.w) \equiv (\forall x.\bigcirc w)$

proof:

1.	$\vdash (\forall x.\bigcirc w) \supset (\bigcirc\forall x.w)$	by *D*4
2.	$\vdash \forall x.w \supset w$	by *D*2
3.	$\vdash (\bigcirc\forall x.w) \supset \bigcirc w$	by $\bigcirc\bigcirc$
4.	$\vdash (\bigcirc\forall x.w) \supset (\forall x.\bigcirc w)$	by $\forall I$
5.	$\vdash (\forall x.\bigcirc w) \equiv (\bigcirc\forall x.w)$	by 1, 4, and *PR*

*T*31. $\vdash (\bigcirc\exists x.w) \equiv (\exists x.\bigcirc w)$

proof:

1.	$\vdash (\forall x.\bigcirc\sim w) \equiv (\bigcirc\forall x.\sim w)$	by *T*30
2.	$\vdash (\forall x.\sim\bigcirc w) \equiv (\bigcirc\sim\exists x.w)$	by *C*4, *D*1, and *ER*
3.	$\vdash (\sim\exists x.\bigcirc w) \equiv (\sim\bigcirc\exists x.w)$	by *C*4, *D*1, and *PR*
4.	$\vdash (\exists x.\bigcirc w) \equiv (\bigcirc\exists x.w)$	by *PR*

Theorem *T*28 implies the commutativity of $\forall$ with $\Box$: Both have a universal character, with one quantifying over individuals and the other quantifying over states. Similarly, Theorem *T*29 implies the commutativity of $\exists$ with $\Diamond$. The last two theorems (*T*30 and *T*31) imply the commutativity of $\forall$ and $\exists$ with $\bigcirc$.

5. EQUALITY

Equality is handled by the following axioms:

Axioms:

*E*1. $\vdash t = t$ for any term t

*E*2. $\vdash (t_1 = t_2) \supset [w(t_1,t_1) \equiv w(t_1,t_2)]$
and t_2 is any term globally free for t_1 in w.

Axiom *E*1 states the ***reflexivity*** of equality. Axiom *E*2 states the ***substitutivity*** property of equality. We use $w(t_1,t_2)$ to indicate that t_2 replaces ***some*** of the occurrences of t_1 in w.

Recall that a term t_2 is said to be ***globally free for*** t_1 in w if substitution of t_2 for all free occurrences of t_1 in w : (a) does not create new bound occurrences of (global) variables, and (b) does not create new occurrences of local variables in the scope of a modal operator.

Note that the classical axiom for substitutivity of equality $E2$

$$\vdash \ (t_1 = t_2) \supset [w(t_1, t_1) \equiv w(t_1, t_2)]$$

(where t_2 is free for t_1 in w) is not correct if w contains modal operators. We could take $w(t_1, t_2)$ to be $\Box(t_1 = t_2)$ and deduce from $E2$

$$\vdash \ (t_1 = t_2) \supset [\Box(t_1 = t_1) \equiv \Box(t_1 = t_2)],$$

i.e.,

$$\vdash \ (t_1 = t_2) \supset \Box(t_1 = t_2),$$

which is not a valid statement (since $t_1 = t_2$ may contain local variables). But we have the following theorem for arbitrary formulas.

T32. Substitutivity of Equality

$$\vdash \ \Box(t_1 = t_2) \supset [w(t_1, t_1) \equiv w(t_1, t_2)]$$

where t_2 is free for t_1 in w.

proof:

By induction on the structure of w.

Case: w contains no modal operators. Then

1. $\vdash \ (t_1 = t_2) \supset [w(t_1, t_1) \equiv w(t_1, t_2)]$ by $E2$
2. $\vdash \ \Box(t_1 = t_2) \supset (t_1 = t_2)$ by $C3$
3. $\vdash \ \Box(t_1 = t_2) \supset [w(t_1, t_1) \equiv w(t_1, t_2)]$ by MP

Case: w is of the form $\Box u$. Then

1. $\vdash \ \Box(t_1 = t_2) \supset [u(t_1, t_1) \equiv u(t_1, t_2)]$ induction hypothesis
2. $\vdash \ \Box(t_1 = t_2)$ assumption
3. $\vdash \ u(t_1, t_1) \equiv u(t_1, t_2)$ by MP
4. $\vdash \ \Box u(t_1, t_1) \equiv \Box u(t_1, t_2)$ by $\Box\Box$

Thus, $\Box(t_1 = t_2) \vdash \ \Box u(t_1, t_1) \equiv \Box u(t_1, t_2)$

4. $\vdash \ \Box\Box(t_1 = t_2) \supset [\Box u(t_1, t_1) \equiv \Box u(t_1, t_2)]$ by DED

5. $\vdash \Box(t_1 = t_2) \supset [\Box u(t_1, t_1) \equiv \Box u(t_1, t_2)]$ by $T2$ and PR

The cases in which w is of the form $\Diamond u$, $\bigcirc u$, $\forall x.u$, and $\exists x.u$ are treated similarly, using the $\Diamond\Diamond$-rule, the $\bigcirc\bigcirc$-rule, the $\forall\forall$-rule, and the $\exists\exists$-rule, respectively.

Case: w is of the form $u \, \mathcal{U} \, v$.

1. $\vdash \Box(t_1 = t_2) \supset [u(t_1, t_1) \equiv u(t_1, t_2)]$ induction hypothesis
2. $\vdash \Box(t_1 = t_2) \supset [v(t_1, t_1) \equiv v(t_1, t_2)]$ induction hypothesis
3. $\vdash \Box(t_1 = t_2)$ assumption
4. $\vdash u(t_1, t_1) \equiv u(t_1, t_2)$ by 1, 3, and MP
5. $\vdash v(t_1, t_1) \equiv v(t_1, t_2)$ by 2, 3, and MP
6. $\vdash [u(t_1, t_1) \, \mathcal{U} \, v(t_1, t_1)] \equiv [u(t_1, t_2) \, \mathcal{U} \, v(t_1, t_2)]$ by 4, 5, and ER

Thus, $\Box(t_1 = t_2) \vdash \big(u(t_1, t_1) \, \mathcal{U} \, v(t_1, t_1)\big) \equiv \big(u(t_1, t_2) \, \mathcal{U} \, v(t_1, t_2)\big)$

7. $\vdash \Box\Box(t_1 = t_2) \supset \big[\big(u(t_1, t_1) \, \mathcal{U} \, v(t_1, t_1)\big) \equiv \big(u(t_1, t_2) \, \mathcal{U} \, v(t_1, t_2)\big)\big]$
by DED
8. $\vdash \Box(t_1 = t_2) \supset \big[\big(u(t_1, t_1) \, \mathcal{U} \, v(t_1, t_1)\big) \equiv \big(u(t_1, t_2) \, \mathcal{U} \, v(t_1, t_2)\big)\big]$
by $T2$ and PR ▮

T33. Commutativity of Equality

$$\vdash (t_1 = t_2) \supset (t_2 = t_1)$$

proof:

1. $\vdash (t_1 = t_2) \supset [(t_1 = t_1) \equiv (t_2 = t_1)]$ by $E2$
2. $\vdash t_1 = t_1$ by $E1$
3. $\vdash (t_1 = t_2) \supset (t_2 = t_1)$ by 1, 2, and PR

T34. Transitivity of Equality

$$\vdash [(t_1 = t_2) \land (t_2 = t_3)] \supset (t_1 = t_3)$$

proof:

1. $\vdash (t_1 = t_2) \supset [(t_1 = t_3) \equiv (t_2 = t_3)]$ by $E2$
2. $\vdash [(t_1 = t_2) \land (t_2 = t_3)] \supset (t_1 = t_3)$ by PR

T35. Term Equality

(a) $\vdash \Box(t_1 = t_2) \supset \big(\tau(t_1) = \tau(t_2)\big)$ for any term τ

(b) $\vdash (t_1 = t_2) \supset \big(\tau(t_1) = \tau(t_2)\big)$ where τ does not contain the next operator.

Here, $\tau(t_2)$ is the result of replacing an occurrence of t_1 in τ by t_2.

proof of (a):

1. $\vdash \;\Box(t_1 = t_2) \;\supset\; [(\tau(t_1) = \tau(t_2)) \;\equiv\; (\tau(t_2) = \tau(t_2))]$ by $T32$
2. $\vdash \;\tau(t_2) = \tau(t_2)$ by $E1$
3. $\vdash \;\Box(t_1 = t_2) \;\supset\; (\tau(t_1) = \tau(t_2))$ by 1, 2, and PR

proof of (b):

1. $\vdash \;(t_1 = t_2) \supset [(\tau(t_1) = \tau(t_2)) \equiv (\tau(t_2) = \tau(t_2))]$ by $E2$ (no $\bigcirc$ in τ)
2. $\vdash \;\tau(t_2) = \tau(t_2)$ by $E1$
3. $\vdash \;(t_1 = t_2) \supset (\tau(t_1) = \tau(t_2))$ by 1, 2, and PR

6. FRAME AXIOMS AND RULES

The use of the next operator $\bigcirc$ applied to terms is governed by the axioms:

Axioms:

$N1.$ $\vdash \;\bigcirc f(t_1, \ldots, t_n) \;=\; f(\bigcirc t_1, \ldots, \bigcirc t_n)$
for any function f and terms $t_1, \ldots, t_n$

$N2.$ $\vdash \;\bigcirc p(t_1, \ldots, t_n) \;\equiv\; p(\bigcirc t_1, \ldots, \bigcirc t_n)$
for any predicate p and terms $t_1, \ldots, t_n$

$N3.$ $\vdash \;\bigcirc(t_1 = t_2) \;\equiv\; (\bigcirc t_1 = \bigcirc t_2)$

Axiom $N3$ is a special case of $N2$ where p is the equality predicate.

These axioms are consistent with the evaluation rules that we gave which stated that to evaluate an expression $\bigcirc\, \mathcal{E}(t_1, \ldots t_n)$, we can evaluate $\mathcal{E}(\bigcirc t_1, \ldots \bigcirc t_n)$ regardless of whether $\mathcal{E}$ is a term or a logical expression.

Recall that we split the set of our symbols into two subsets: global and local symbols. The logical consequence of this convention is the following frame axiom:

FA. *Frame Axiom*
$\vdash x = \bigcirc x$ for every global variable x

We can therefore prove by induction on the structure of the term t and the formula w the following *frame theorems*:

T36. For a term t and formula w

(*a*) $\vdash t = \bigcirc t$ provided t does not contain local symbols

(*b*) $\vdash w \equiv \Box w$ provided w does not contain local symbols

(*c*) $\vdash w(\bigcirc y_1, \ldots, \bigcirc y_n) \equiv \bigcirc w(y_1, \ldots, y_n)$
provided $y_1, \ldots, y_n$ are all the local variables in w.

A derived frame rule that we will be using is

Frame Rule - FR

$$\frac{\vdash \; w_1 \supset \Diamond w_2}{\vdash \; (w \wedge w_1) \; \supset \; \Diamond(w \wedge w_2)}$$

provided w does not contain local symbols.

proof:

1. $\vdash \; w \supset \Box w$ by *T36*
2. $\vdash \; w_1 \supset \Diamond w_2$ given
3. $\vdash \; (w \wedge w_1) \supset (\Box w \wedge \Diamond w_2)$ by 1, 2, and *PR*
4. $\vdash \; (\Box w \wedge \Diamond w_2) \supset \Diamond(w \wedge w_2)$ by *T10*
5. $\vdash \; (w \wedge w_1) \supset \Diamond(w \wedge w_2)$ by 3, 4, and *PR*

7. DOMAIN PART

The next part of the system contains domain axioms that specify the necessary properties of the domain of interest. Thus, to reason about programs manipulating natural numbers, we need the set of Peano Axioms, and to reason about trees we need a set of axioms giving the basic properties of trees and the basic operations defined on them.

An essential axiom schema for many domains is the ***induction axiom schema***. This (and all other schemas) should be formulated to admit modal instances as subformulas. Thus the induction principle for natural numbers can be stated as follows:

Induction Axiom

$$\vdash \; [R(0) \; \wedge \; \forall n(R(n) \; \supset \; R(n+1))] \; \supset \; R(k)$$

for any statement R.

One instance of this principle, which will be used later, is obtained by taking $R(n)$ to be $\Box(Q(n) \supset \Diamond \psi)$:

Induction Theorem

$$\begin{aligned} \vdash\ & \{\Box(Q(0) \supset \Diamond\psi) \\ & \quad \wedge\ \forall n[\Box(Q(n) \supset \Diamond\psi) \supset \Box(Q(n+1) \supset \Diamond\psi)]\} \\ & \qquad \supset\ \Box(Q(k) \supset \Diamond\psi). \end{aligned}$$

Similar induction theorems exist for other domains and depend on well-founded orderings existing in those domains.

Using this induction theorem we can derive the following useful induction rule:

Induction Rule – IND

$$\frac{\begin{array}{l} \vdash\ Q(0) \supset \Diamond\psi \\ \vdash\ Q(n+1) \supset (\Diamond\psi \vee \Diamond Q(n)) \end{array}}{\vdash\ Q(k) \supset \Diamond\psi}$$

IND is useful for proving convergence of a loop: Show that $Q(0)$ guarantees $\Diamond\psi$ and that for each n, either $Q(n+1)$ implies $Q(n)$ across the loop or it already establishes $\Diamond\psi$ and no further execution is necessary. Then $Q(k)$ ensures that the loop is executed ***at most k*** times and that $\Diamond\psi$ is established on the last iteration or earlier.

proof:

1. $\vdash\ Q(0) \supset \Diamond\psi$ — given

2. $\vdash\ \Box(Q(0) \supset \Diamond\psi)$ — by $\Box I$

3. $\vdash\ Q(n+1) \supset (\Diamond\psi \vee \Diamond Q(n))$ — given

4. $\vdash\ \Box(Q(n) \supset \Diamond\psi) \supset (\Diamond Q(n) \supset \Diamond\psi)$ — by *T*5, *T*3 and *PR*

5. $\vdash\ [(\Diamond Q(n) \supset \Diamond\psi) \wedge (\Diamond\psi \vee \Diamond Q(n))] \supset \Diamond\psi$ — by *PT*

6. $\vdash\ [Q(n+1) \wedge \Box(Q(n) \supset \Diamond\psi)] \supset \Diamond\psi$ — by 3, 4, 5 and *PR*

7. $\vdash\ \Box(Q(n) \supset \Diamond\psi) \supset (Q(n+1) \supset \Diamond\psi)$ — by *PR*

8. $\vdash\ \Box\Box(Q(n) \supset \Diamond\psi) \supset \Box(Q(n+1) \supset \Diamond\psi)$ — by $\Box\Box$

9. $\vdash\ \Box(Q(n) \supset \Diamond\psi) \supset \Box(Q(n+1) \supset \Diamond\psi)$ — by *T*2 and *PR*

10. $\vdash\ \forall n[\Box(Q(n) \supset \Diamond\psi) \supset \Box(Q(n+1) \supset \Diamond\psi)]$ — by $\forall I$

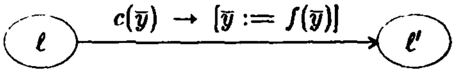
11. $\vdash\ \Box(Q(k) \supset \Diamond\psi)$ — by 2, 10, and Induction Theorem

12. $\vdash\ Q(k) \supset \Diamond\psi$ — by *C*3 and *MP* ∎

8. PROGRAM PART

Our proof system must be augmented by additional axioms that reflect the structure of the program under consideration. These additional axioms constrain the state sequences to be exactly the set of execution sequences of the program under study. This releases us from the need to express program text syntactically in the system; all necessary information is captured by constraints on the accessibility relation that are expressed by the additional axioms.

For simplicity, we assume that the program is represented by a directed graph whose nodes are the program locations or labels and whose edges represent transitions between the labels. A transition is an instruction of the general form



Here, $c(\bar{y})$ is a condition (possibly the trivial condition ***true***) under which the transition replacing $\bar{y}$ by $f(\bar{y})$ should be taken, where $\bar{y} = (y_1, \ldots, y_n)$ is the vector of program variables.

We assume that the programs are sequential and deterministic; in other words, all the conditions $c_1, \ldots, c_k$ on transitions departing from any node are ***exhaustive***, *i.e.*, $\bigvee_{i=1}^{k} c_i(\bar{y}) = \textit{true}$, and ***mutually exclusive***. In order to uniformly satisfy this requirement we add "***true*** → [ ]" self-*transitions* to all the exit nodes.

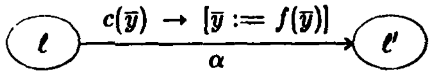
A first generic axiom states that in every state s, ***at*** ℓ is true for exactly one label ℓ. Let L denote the set of all labels in the program; we have

Location Axiom – *LA*

$$\vdash \sum_{\ell \in L} \textit{at}\,\ell = 1.$$

We use here the abbreviation $\sum p_i = 1$ or $p_1 + \cdots + p_n = 1$ to mean that ***exactly*** one of the p_i's is true; $p_i = 1$ if p_i is true and $p_i = 0$ if p_i is false.

The role of the other axioms, called the ***transition axioms***, is to introduce our knowledge about the program into the system. Since the system does not provide direct tools for speaking about programs (such as mentioning program text in Hoare's formalism or Dynamic Logic), the transition axioms represent the program by characterizing the possible state transitions under the execution of the program. For any transition:



we generate a transition axiom F_α. This axiom corresponds to a "forward" propagation (***symbolic execution***) across the transition α:

Forward transition axiom

$F_\alpha: \ \vdash \ [at\,\ell \wedge c(\overline{y}) \wedge \overline{y} = \overline{u}] \ \supset \ \bigcirc[at\,\ell' \wedge \overline{y} = f(\overline{u})]$,

where $\overline{u}$ are auxiliary global variables.

This axiom states: If at any state, execution is at ℓ, $c(\overline{y})$ holds, and the current values of $\overline{y}$ are $\overline{u}$, then at the next state we will be at ℓ' with $\overline{y} = f(\overline{u})$.

A different approach that suggests an alternative axiom schema is obtained by "backward" substitution (derivation of the *weakest precondition*)

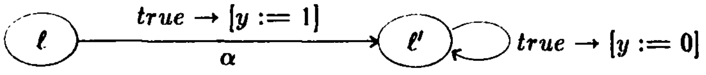
Backward transition axiom

$B_\alpha: \ \vdash \ [at\,\ell \wedge c(\overline{y}) \wedge P(f(\overline{y}))] \ \supset \ \bigcirc[at\,\ell' \wedge P(\overline{y})]$,

where P is any state predicate (*i.e.*, without modalities).

Here $P(f(\overline{y}))$ denotes the substitution of $f(\overline{y})$ for all free occurrences of $\overline{y}$ in $P(\overline{y})$. This form of the axiom expresses the effect of the transition on an arbitrary "state" predicate P; *i.e.*, a predicate P that does not contain any modal operators. It says that if $at\,\ell \wedge c(\overline{y})$ and $P(f(\overline{y}))$ hold, then we are guaranteed to reach ℓ' with $P(\overline{y})$ on the next step.

The predicate P may not contain modalities. As a counterexample, consider the program segment



with

$$P(y): \quad \Box(y = 1).$$

The appropriate instance of the backward axiom for α is

$$B_\alpha: \ \vdash \ [at\,\ell \wedge true \wedge \Box(1 = 1)] \ \supset \ \bigcirc[at\,\ell' \wedge \Box(y = 1)],$$

which clearly does not correctly reflect the computation of the program.

F_α and B_α are equivalent and can be derived from each other. That is

For every transition α:

B_α holds for every P if and only if F_α holds

proof: B_α for every $P \Rightarrow F_\alpha$.

1. $\vdash \ [at\,\ell \wedge c(\overline{y}) \wedge P(f(\overline{y}))] \ \supset \ \bigcirc[at\,\ell' \wedge P(\overline{y})]$ by B_α, given

2. $\vdash \ [at\,\ell \wedge c(\bar{y}) \wedge f(\bar{y}) = f(\bar{u})] \supset \bigcirc[at\,\ell' \wedge \bar{y} = f(\bar{u})]$
taking $P(\bar{y})$ to be $\bar{y} = f(\bar{u})$,
where $\bar{u}$ are auxiliary global variables

3. $\vdash \ [at\,\ell \wedge c(\bar{y}) \wedge \bar{y} = \bar{u}] \supset [at\,\ell \wedge c(\bar{y}) \wedge f(\bar{y}) = f(\bar{u}$
by $T35(b)$ and PR

4. $\vdash \ [at\,\ell \wedge c(\bar{y}) \wedge \bar{y} = \bar{u}] \supset \bigcirc[at\,\ell' \wedge \bar{y} = f(\bar{u})]$
by 2, 3 and PR

which is the desired F_α. ▮

proof: $F_\alpha \Rightarrow B_\alpha$ for every P.

Let P be an arbitrary state predicate and $\bar{u}$ auxiliary global variables not in P. Then

1. $\vdash \ [at\,\ell \wedge c(\bar{y}) \wedge \bar{y} = \bar{u}] \supset \bigcirc[at\,\ell' \wedge \bar{y} = f(\bar{u})]$ — F_α, given

2. $\vdash \ \bigcirc[at\,\ell' \wedge \bar{y} = f(\bar{u})] \supset [\bigcirc\, at\,\ell' \wedge \bigcirc(\bar{y} = f(\bar{u}))]$ — by $T13$

3. $\vdash \ \bigcirc(\bar{y} = f(\bar{u})) \supset ((\bigcirc\,\bar{y}) = f(\bigcirc\,\bar{u}))$ — by $N3$ and $N1$

4. $\vdash \ \bar{u} = \bigcirc\,\bar{u}$ — by FA, since $\bar{u}$ is global

5. $\vdash \ f(\bar{u}) = f(\bigcirc\,\bar{u})$ — by $T35(b)$

6. $\vdash \ \bigcirc(\bar{y} = f(\bar{u})) \supset ((\bigcirc\,\bar{y}) = f(\bar{u}))$ — by 3, 5, $E2$, and PR

7. $\vdash \ [at\,\ell \wedge c(\bar{y}) \wedge \bar{y} = \bar{u}] \supset [\bigcirc\, at\,\ell' \wedge (\bigcirc\,\bar{y}) = f(\bar{u})]$
by 1, 2, 6, and PR

8. $\vdash \ [\bar{y} = \bar{u} \wedge P(f(\bar{y}))] \supset P(f(\bar{u}))$ — by $E2$ (no modal operators in P) and PR

9. $\vdash \ [at\,\ell \wedge c(\bar{y}) \wedge \bar{y} = \bar{u} \wedge P(f(\bar{y}))]$
$\supset [\bigcirc\, at\,\ell' \wedge (\bigcirc\,\bar{y}) = f(\bar{u}) \wedge P(f(\bar{u}))]$ — by 7, 8, and PR

10. $\vdash \ ((\bigcirc\,\bar{y}) = f(\bar{u})) \supset (P(\bigcirc\,\bar{y}) \equiv P(f(\bar{u})))$ — by $E2$ and PR

11. $\vdash \ P(\bigcirc\,\bar{y}) \equiv \bigcirc\,P(\bar{y})$ — by $T36(c)$

12. $\vdash \ [(\bigcirc\,\bar{y}) = f(\bar{u}) \wedge P(f(\bar{u}))] \supset \bigcirc\,P(\bar{y})$ — by 10, 11, and PR

13. $\vdash \ [at\,\ell \wedge c(\bar{y}) \wedge \bar{y} = \bar{u} \wedge P(f(\bar{y}))] \supset [\bigcirc\, at\,\ell' \wedge \bigcirc\,P(\bar{y})]$
by 9, 12, and PR

14. $\vdash \ [at\,\ell \wedge c(\bar{y}) \wedge \bar{y} = \bar{y} \wedge P(f(\bar{y}))] \supset [\bigcirc\, at\,\ell' \wedge \bigcirc\,P(\bar{y})]$
by $INST$

15. $\vdash \ [at\,\ell \wedge c(\bar{y}) \wedge P(f(\bar{y}))] \supset [\bigcirc\, at\,\ell' \wedge \bigcirc\,P(\bar{y})]$ — by $E1$ and PR

16. $\vdash \ [at\,\ell \wedge c(\bar{y}) \wedge P(f(\bar{y}))] \supset \bigcirc[at\,\ell' \wedge P(\bar{y})]$ — by $T13$ and PR

which is the desired B_α. ▮

We often use a weaker form of the transition axioms:

$$F'_\alpha : \quad \vdash \; [at\,\ell \wedge c(\overline{y}) \wedge \overline{y} = \overline{u}] \;\supset\; \Diamond[at\,\ell' \wedge \overline{y} = f(\overline{u})]$$

and

$$B'_\alpha : \quad \vdash \; [at\,\ell \wedge c(\overline{y}) \wedge P(f(\overline{y}))] \;\supset\; \Diamond[at\,\ell' \wedge P(\overline{y})]$$

obtained from F_α and B_α, respectively, by replacing $\bigcirc$ with $\Diamond$. The weaker forms follow by $T11$, *i.e.* $\vdash \bigcirc w \supset \Diamond w$.

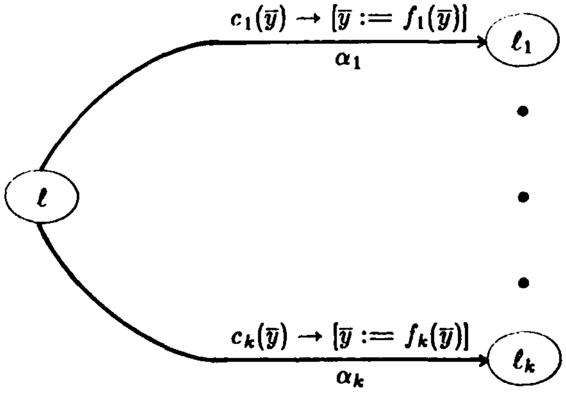
9. THE INVARIANCE PRINCIPLE

We now present a general method for proving invariance properties of programs, *i.e.*, properties that hold continuously throughout the execution. Such properties are expressible by formulas of form

$$\vdash \; [at\,\ell_0 \wedge \phi(\overline{x})] \;\supset\; \Box Q(\overline{y}).$$

That is, $Q(\overline{y})$ is invariantly true for every computation starting at ℓ_0 with input $\overline{x}$ satisfying the precondition $\phi(\overline{x})$.

Let ℓ be any label in the program under consideration and let its outgoing transitions be of the form


$c_1(\overline{y}) \to [\overline{y} := f_1(\overline{y})]$
α_1
ℓ_1
ℓ
$c_k(\overline{y}) \to [\overline{y} := f_k(\overline{y})]$
α_k
ℓ_k

Recall that we assume that $c_1(\overline{y}), \ldots, c_k(\overline{y})$ are exhaustive, *i.e.* $\bigvee_{i=1}^{k} c_i(\overline{y}) = true$, and mutually exclusive. We denote by L the set of all labels in P. We have

Invariance Principle:

Let $Q(\bar{y})$ be a state predicate (with no modalities) and labels describing a property of program P with input condition $\phi(\bar{x})$.

If

(a) Q is true initially, *i.e.*,

$$\vdash \; [at\,\ell_0 \;\wedge\; \phi(\bar{x})] \;\supset\; Q(\bar{y})$$

(b) Q is maintained along any transition α in P, *i.e.*,

$$\vdash \; [at\,\ell \;\wedge\; c_\alpha(\bar{y}) \;\wedge\; Q(\bar{y})] \;\supset\; Q(f_\alpha(\bar{y})),$$

then Q is invariantly true, *i.e.*,

$$\vdash \; [at\,\ell_0 \;\wedge\; \phi(\bar{x})] \;\supset\; \Box Q(\bar{y}).$$

proof:

Consider an arbitrary label ℓ and an arbitrary transition α_i, $1 \leq i \leq k$, from ℓ to ℓ_i.

1. $\vdash \; [at\,\ell \;\wedge\; c_i(\bar{y}) \;\wedge\; Q(\bar{y})] \;\supset\; [at\,\ell \;\wedge\; c_i(\bar{y}) \;\wedge\; Q(f_i(\bar{y}))]$ — by (b) and *PR*
2. $\vdash \; [at\,\ell \;\wedge\; c_i(\bar{y}) \;\wedge\; Q(f_i(\bar{y}))] \;\supset\; \bigcirc[at\,\ell_i \;\wedge\; Q(\bar{y})]$ — by B_{α_i}
3. $\vdash \; [at\,\ell \;\wedge\; c_i(\bar{y}) \;\wedge\; Q(\bar{y})] \;\supset\; \bigcirc[at\,\ell_i \;\wedge\; Q(\bar{y})]$ — by 1, 2 and *PR*
4. $\vdash \; [at\,\ell \;\wedge\; c_i(\bar{y}) \;\wedge\; Q(\bar{y})] \;\supset\; \bigcirc Q(\bar{y})$ — by *T*13 and *PR*

5. $\vdash \; \bigvee_{i=1}^{k}[at\,\ell \;\wedge\; c_i(\bar{y}) \;\wedge\; Q(\bar{y})] \;\supset\; \bigcirc Q(\bar{y})$ — by *PR* (taking the disjunction over all transitions from ℓ)
6. $\vdash \; [at\,\ell \;\wedge\; \bigvee_{i=1}^{k} c_i(\bar{y}) \;\wedge\; Q(\bar{y})] \;\supset\; \bigcirc Q(\bar{y})$ — by *PR*
7. $\vdash \; \bigvee_{i=1}^{k} c_i(\bar{y}) \;=\; true$ — assumption
8. $\vdash \; [at\,\ell \;\wedge\; Q(\bar{y})] \;\supset\; \bigcirc Q(\bar{y})$ — by *PR*

9. $\vdash \; \bigvee_{\ell \in L}[at\,\ell \;\wedge\; Q(\bar{y})] \;\supset\; \bigcirc Q(\bar{y})$ — by *PR* (taking the disjunction over all labels of P)
10. $\vdash \; [(\bigvee_{\ell \in L} at\,\ell) \;\wedge\; Q(\bar{y})] \;\supset\; \bigcirc Q(\bar{y})$ — by *PR*
11. $\vdash \; \bigvee_{\ell \in L} at\,\ell \;=\; true$ — by Location Axiom and *PR*
12. $\vdash \; Q(\bar{y}) \;\supset\; \bigcirc Q(\bar{y})$ — by 10, 11 and *PR*

13. $\vdash \; Q(\bar{y}) \;\supset\; \Box Q(\bar{y})$ — by *CI*

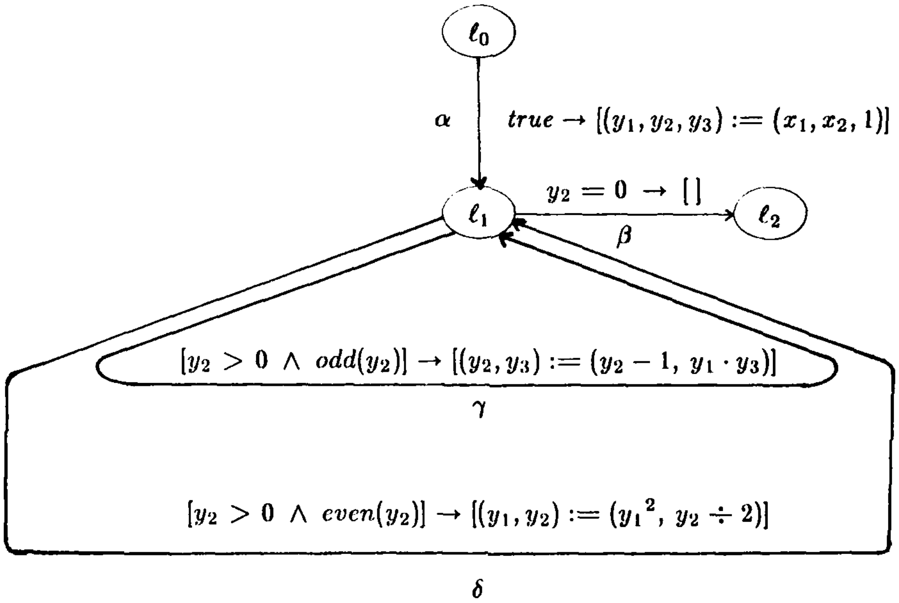
14. $\vdash \ [at\,\ell_0 \ \wedge \ \phi(\overline{x})] \ \supset \ Q(\overline{y})$ by (a)

15. $\vdash \ [at\,\ell_0 \ \wedge \ \phi(\overline{x})] \ \supset \ \Box Q(\overline{y})$ by 13, 14 and *PR*

10. EXAMPLE: INTEGER EXPONENTIATION PROGRAM

Consider for example the following program *IE* over the integers, which raises a real number x_1 to an integer x_2, *i.e.* $x_1{}^{x_2}$, where $x_2 \geq 0$. We assume that $0^0 = 1$.

Program IE (Integer Exponentiation):



ℓ_0
α
$true \rightarrow [(y_1, y_2, y_3) := (x_1, x_2, 1)]$
$y_2 = 0 \rightarrow [\,]$
ℓ_1
ℓ_2
β
$[y_2 > 0 \ \wedge \ odd(y_2)] \rightarrow [(y_2, y_3) := (y_2 - 1, \ y_1 \cdot y_3)]$
γ
$[y_2 > 0 \ \wedge \ even(y_2)] \rightarrow [(y_1, y_2) := (y_1{}^2, \ y_2 \div 2)]$
δ

Let

$$\phi: \ at\,\ell_0 \ \wedge \ x_2 \geq 0$$

$$\psi: \ at\,\ell_2 \ \wedge \ y_3 = x_1{}^{x_2}.$$

We would like to use our proof system to establish the total correctness of program *IE* with respect to ϕ and ψ; we will show

$$\vdash \ \phi \ \supset \ \Diamond \psi.$$

In the proof we ignore type considerations such as $real(x_1)$ and $integer(x_2)$. (See [BUR], [MW]).

PROOF 1: Using Backward Transition Axioms

The backward transition axiom schemata corresponding to this program (taking the weaker form, with $\Diamond$ rather than $\bigcirc$) are:

$$B'_\alpha: \quad \vdash \ [at\,\ell_0 \ \wedge \ P(x_1, x_2, 1)] \ \supset \ \Diamond[at\,\ell_1 \ \wedge \ P(y_1, y_2, y_3)]$$

$$B'_\beta: \quad \vdash \ [at\,\ell_1 \wedge y_2 = 0 \wedge P(y_1, y_2, y_3)] \supset \Diamond[at\,\ell_2 \wedge P(y_1, y_2, y_3)]$$

$$B'_\gamma: \quad \vdash \ [at\,\ell_1 \wedge y_2 > 0 \wedge odd(y_2) \wedge P(y_1,\ y_2 - 1,\ y_1 \cdot y_3)] \\ \supset \Diamond[at\,\ell_1 \wedge P(y_1, y_2, y_3)]$$

$$B'_\delta: \quad \vdash \ [at\,\ell_1 \wedge y_2 > 0 \wedge even(y_2) \wedge P({y_1}^2,\ y_2 \div 2,\ y_3)] \\ \supset \Diamond[at\,\ell_1 \wedge P(y_1, y_2, y_3)].$$

We prove

$(a) \quad \vdash \phi \supset \Diamond\, \exists k.Q(k, \overline{y})$

$(b) \quad \vdash (\exists k.Q(k, \overline{y})) \supset \Diamond\, \psi$, or equivalently $\vdash Q(k, \overline{y}) \supset \Diamond\, \psi$,

where

$$Q(n, \overline{y}): \quad at\,\ell_1 \ \wedge \ (0 \leq y_2 \leq n) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}.$$

Here, $0 \leq y_2 \leq n$ is used to establish the termination, and $y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}$ is the invariant used to establish the correctness.

Clearly, by rule $\Diamond\, C$, parts (a) and (b) imply the desired result $\vdash \phi \supset \Diamond\, \psi$.

proof of (a):

1. $\vdash \ 1 \cdot {x_1}^{x_2} = {x_1}^{x_2}$ by domain

2. $\vdash \ \phi \ \supset \ [at\ \ell_0 \wedge x_2 \geq 0 \wedge 1 \cdot {x_1}^{x_2} = {x_1}^{x_2}]$ by PR

3. $\vdash \ [at\ \ell_0 \wedge x_2 \geq 0 \wedge 1 \cdot {x_1}^{x_2} = {x_1}^{x_2}]$
   $\supset \ \Diamond[at\,\ell_1 \wedge y_2 \geq 0 \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}]$ by B'_α
   where P is $y_2 \geq 0 \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}$

4. $\vdash \ (y_2 \geq 0) \supset (0 \leq y_2 \leq y_2)$ by domain

5. $\vdash \ [at\,\ell_1 \wedge y_2 \geq 0 \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}]$
   $\supset \ [at\,\ell_1 \wedge (0 \leq y_2 \leq y_2) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}]$ by 4 and PR

6. $\vdash \ [at\,\ell_1 \wedge y_2 \geq 0 \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}]$
   $\supset \ \exists k[at\,\ell_1 \wedge (0 \leq y_2 \leq k) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}]$ by $T24$

7. $\vdash \ \phi \ \supset \ \Diamond\, \exists k.Q(k, \overline{y})$ by 2, 3, 6 and $\Diamond\, Q$

proof of (b): We use the induction rule *IND*:

$$\begin{array}{l} (b_1) \quad \vdash Q(0, \overline{y}) \ \supset \ \Diamond\, \psi \\ (b_2) \quad \vdash Q(n+1, \overline{y}) \ \supset \ [\Diamond\, \psi \vee \Diamond\, Q(n, \overline{y})] \\ \hline \qquad\quad \vdash Q(k, \overline{y}) \ \supset \ \Diamond\, \psi \end{array}$$

proof of (b_1):

8. $\vdash\ [(0 \leq y_2 \leq 0) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}] \supset [y_2 = 0 \wedge y_3 = {x_1}^{x_2}]$
   by domain

9. $\vdash\ Q(0, \bar{y}) \supset [at\,\ell_1 \wedge y_2 = 0 \wedge y_3 = {x_1}^{x_2}]$
   by PR

10. $\vdash\ [at\,\ell_1 \wedge y_2 = 0 \wedge y_3 = {x_1}^{x_2}] \supset \Diamond[at\,\ell_2 \wedge y_3 = {x_1}^{x_2}]$
    by B'_β, where P is $y_3 = {x_1}^{x_2}$

11. $\vdash\ Q(0, \bar{y}) \supset \Diamond\psi$ by 9, 10 and PR

proof of (b_2):

case 1: $y_2 = 0$.

12. $\vdash\ [y_2 = 0 \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}] \supset [y_2 = 0 \wedge y_3 = {x_1}^{x_2}]$
    by domain

13. $\vdash\ [Q(n+1, \bar{y}) \wedge y_2 = 0] \supset [at\,\ell_1 \wedge y_2 = 0 \wedge y_3 = {x_1}^{x_2}]$
    by PR

14. $\vdash\ [at\,\ell_1 \wedge y_2 = 0 \wedge y_3 = {x_1}^{x_2}] \supset \Diamond[at\,\ell_2 \wedge y_3 = {x_1}^{x_2}]$
    by B'_β, where P is $y_3 = {x_1}^{x_2}$

15. $\vdash\ [Q(n+1, \bar{y}) \wedge y_2 = 0] \supset \Diamond\psi$ by 13, 14 and PR

case 2: $y_2 > 0 \wedge odd(y_2)$.

16. $\vdash\ [y_2 > 0 \wedge (0 \leq y_2 \leq n+1) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}]$
    $\supset [(0 \leq y_2 - 1 \leq n) \wedge (y_1 \cdot y_3) \cdot {y_1}^{y_2 - 1} = {x_1}^{x_2}]$
    by domain

17. $\vdash\ [Q(n+1, \bar{y}) \wedge y_2 > 0 \wedge odd(y_2)] \supset [at\,\ell_1 \wedge y_2 > 0 \wedge odd(y_2)$
    $\wedge (0 \leq y_2 - 1 \leq n) \wedge (y_1 \cdot y_3) \cdot {y_1}^{y_2 - 1} = {x_1}^{x_2}]$
    by PR

18. $\vdash\ [at\,\ell_1 \wedge y_2 > 0 \wedge odd(y_2) \wedge (0 \leq y_2 - 1 \leq n) \wedge (y_1 \cdot y_3) \cdot {y_1}^{y_2 - 1} = {x_1}^{x_2}]$
    $\supset \Diamond[at\,\ell_1 \wedge (0 \leq y_2 \leq n) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}]$
    by B'_γ, where P is $(0 \leq y_2 \leq n) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}$

19. $\vdash\ [Q(n+1, \bar{y}) \wedge y_2 > 0 \wedge odd(y_2)] \supset \Diamond Q(n, \bar{y})$
    by 17, 18, and PR

case 3: $y_2 > 0 \wedge even(y_2)$.

20. $\vdash\ [even(y_2) \wedge (0 \leq y_2 \leq n+1) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}]$
    $\supset [(0 \leq y_2 \div 2 \leq n) \wedge y_3 \cdot ({y_1}^2)^{y_2 \div 2} = {x_1}^{x_2}]$
    by domain

21. $\vdash\ [Q(n+1,\overline{y})\ \land\ y_2 > 0\ \land\ even(y_2)]\ \supset\ [at\,\ell_1\ \land\ y_2 > 0$
$\land\ even(y_2)\ \land\ (0 \le y_2 \div 2 \le n) \land\ y_3 \cdot (y_1{}^2)^{y_2 \div 2} = x_1{}^{x_2}]$

by PR

22. $\vdash\ [at\,\ell_1\ \land\ y_2 > 0\ \land\ even(y_2)\ \land\ (0 \le y_2 \div 2 \le n)\ \land\ y_3 \cdot (y_1{}^2)^{y_2 \div 2} = x_1{}^{x_2}]$
$\supset\ \Diamond[at\,\ell_1\ \land\ (0 \le y_2 \le n)\ \land\ y_3 \cdot y_1{}^{y_2} = x_1{}^{x_2}]$

by B'_δ, where P is $(0 \le y_2 \le n)\ \land\ (y_3 \cdot y_1{}^{y_2} = x_1{}^{x_2})$

23. $\vdash\ [Q(n+1,\overline{y})\ \land\ y_2 > 0\ \land\ even(y_2)]\ \supset\ \Diamond Q(n,\overline{y})$

by 21, 22, and PR

To summarize, we showed

15. $\vdash\ [Q(n+1,\overline{y})\ \land\ y_2 = 0]\ \supset\ \Diamond\psi$ case 1

19. $\vdash\ [Q(n+1,\overline{y})\ \land\ y_2 > 0\ \land\ odd(y_2)]\ \supset\ \Diamond Q(n,\overline{y})$ case 2

23. $\vdash\ [Q(n+1,\overline{y})\ \land\ y_2 > 0\ \land\ even(y_2)]\ \supset\ \Diamond Q(n,\overline{y})$ case 3

Then since

24. $\vdash\ Q(n+1,\overline{y})\ \supset\ [y_2 = 0\ \lor\ (y_2 > 0 \land odd(y_2))\lor(y_2 > 0 \land even(y_2))]$

by domain

it follows that

25. $\vdash\ Q(n+1,\overline{y})\ \supset\ [\Diamond\psi\ \lor\ \Diamond Q(n,\overline{y})]$

by 15, 19, 23, 24 and PR

This concludes the first proof of the total correctness of our example. ∎

PROOF 2: Using Forward Transition Axioms

For comparison, let us now prove the total correctness of program IE using the forward transition axioms. The proof turns out to be longer than the previous one using the backward axioms.

The forward transition axiom schemas corresponding to the program (taking again the weaker form, with $\Diamond$ rather than $\bigcirc$) are:

$F'_\alpha:\ \vdash\ at\,\ell_0\ \supset\ \Diamond[at\,\ell_1\ \land\ \overline{y} = (x_1, x_2, 1)]$

$F'_\beta:\ \vdash\ [at\,\ell_1\ \land\ y_2 = 0\ \land\ \overline{y} = \overline{u}]\ \supset\ \Diamond[at\,\ell_2\ \land\ \overline{y} = \overline{u}]$

$F'_\sigma:\ \vdash\ [at\,\ell_1\ \land\ y_2 > 0\ \land\ odd(y_2)\ \land\ \overline{y} = \overline{u}]\ \supset\ \Diamond[at\,\ell_1\ \land\ \overline{y} = (u_1, u_1 - 1, u_1 \cdot u_3)]$

$F'_\delta:\ \vdash\ [at\,\ell_1\ \land\ y_2 > 0\ \land\ even(u_2)\ \land\ \overline{y} = \overline{u}]\ \supset\ \Diamond[at\,\ell_1\ \land\ \overline{y} = (u_1{}^2, u_2 \div 2, u_3)]$

Again, let

$$\phi: \quad at\,\ell_0 \ \wedge\ x_2 \geq 0$$

$$\psi: \quad at\,\ell_2 \ \wedge\ y_3 = x_1{}^{x_2}.$$

we would like to establish the total correctness of the program, *i.e.*,

$$\vdash \phi \supset \Diamond \psi.$$

As before, we prove

(*a*) $\vdash \phi \supset \Diamond \exists k. Q(k, \bar{y})$

(*b*) $\vdash (\exists k. Q(k, \bar{y})) \supset \Diamond \psi,$ or equivalently, $\vdash Q(k, \bar{y}) \supset \Diamond \psi,$

where

$$Q(n, \bar{y}): \qquad at\,\ell_1 \ \wedge\ (0 \leq y_2 \leq n) \ \wedge\ y_3 \cdot y_1{}^{y_2} = x_1{}^{x_2}.$$

Parts (*a*) and (*b*) implies the desired result $\vdash \phi \supset \Diamond \psi$ by rule $\Diamond C$. We proceed to prove (*a*) and (*b*).

proof of (*a*):

1. $\vdash \ at\,\ell_0 \ \supset\ \Diamond[at\,\ell_1 \ \wedge\ \bar{y} = (x_1, x_2, 1)]$ — by F'_α

2. $\vdash \ [at\,\ell_0 \ \wedge\ x_2 \geq 0] \ \supset\ \Diamond[at\,\ell_1 \ \wedge\ \bar{y} = (x_1, x_2, 1) \ \wedge\ x_2 \geq 0]$ — by FR

3. $\vdash \ x_2 \geq 0 \ \supset\ [1 \cdot x_1{}^{x_2} = x_1{}^{x_2} \ \wedge\ (0 \leq x_2 \leq x_2)]$ — by domain

4. $\vdash \ [\bar{y} = (x_1, x_2, 1) \ \wedge\ 1 \cdot x_1{}^{x_2} = x_1{}^{x_2} \ \wedge\ (0 \leq x_2 \leq x_2)]$
   $\supset\ [y_3 \cdot y_1{}^{y_2} = x_1{}^{x_2} \ \wedge\ (0 \leq y_2 \leq y_2)]$ — by $E2$ and PR

5. $\vdash \ [at\,\ell_1 \ \wedge\ \bar{y} = (x_1, x_2, 1) \ \wedge\ x_2 \geq 0]$
   $\supset\ [at\,\ell_1 \ \wedge\ y_3 \cdot y_1{}^{y_2} = x_1{}^{x_2} \ \wedge\ (0 \leq y_2 \leq y_2)]$ — by 3, 4, and PR

6. $\vdash \ [at\,\ell_1 \ \wedge\ y_3 \cdot y_1{}^{y_2} = x_1{}^{x_2} \ \wedge\ (0 \leq y_2 \leq y_2)]$
   $\supset\ \exists k[at\,\ell_1 \ \wedge\ y_3 \cdot y_1{}^{y_2} = x_1{}^{x_2} \ \wedge\ (0 \leq y_2 \leq k)]$ — by $T24$

7. $\vdash \ [at\,\ell_0 \ \wedge\ x_2 \geq 0] \ \supset\ \Diamond \exists k[at\,\ell_1 \ \wedge\ y_3 \cdot y_1{}^{y_2} = x_1{}^{x_2} \ \wedge\ (0 \leq y_2 \leq k)]$
   by 2, 5, 6, $\Diamond Q$ and PR

i.e.,

7′. $\vdash \ \phi \ \supset\ \Diamond \exists k. Q(k, \bar{y}).$

proof of (*b*): We use the induction rule *IND*:

$$\begin{array}{l}
(b_1) \quad \vdash \quad Q(0,\overline{y}) \;\supset\; \Diamond\psi \\[4pt]
(b_2) \quad \vdash \quad Q(n+1,\overline{y}) \;\supset\; [\Diamond\psi \lor \Diamond Q(n,\overline{y})] \\
\hline
\vdash \quad Q(k,\overline{y}) \;\supset\; \Diamond\psi
\end{array}$$

In our proof we use the special consequence rule

Consequence $\exists\Diamond$ *rule* – $\exists\Diamond Q$

$$\begin{array}{l}
\vdash \; w_1 \supset \exists u.w_2 \\
\vdash \; w_2 \supset \Diamond w_3 \\
\vdash \; w_3 \supset w_4 \\
\hline
\vdash \; w_1 \supset \Diamond w_4
\end{array}$$

where u is not free in w_4.

proof of rule:

(1) $\vdash \; w_1 \;\supset\; \exists u.w_2$ given

(2) $\vdash \; w_2 \;\supset\; \Diamond w_3$ given

(3) $\vdash \; \exists u.w_2 \;\supset\; \exists u.\Diamond w_3$ by $\exists\exists$

(4) $\vdash \; \exists u.w_2 \;\supset\; \Diamond\exists u.w_3$ by $T29$ and PR

(5) $\vdash \; w_3 \;\supset\; w_4$ given

(6) $\vdash \; \exists u.w_3 \;\supset\; w_4$ by $\exists I$, since u not free in w_4

(7) $\vdash \; w_1 \;\supset\; \Diamond w_4$ by (1), (4), (6), and $\Diamond Q$

proof of (b_1):

8. $\vdash \; (0 \le y_2 \le 0) \supset (y_2 = 0)$ by domain

9. $\vdash \; Q(0,\overline{y}) \supset [at\,\ell_1 \land \overline{y} = \overline{y} \land y_2 = 0 \land y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}]$
by $E1$ and PR

10. $\vdash \; Q(0,\overline{y}) \supset \exists\overline{u}.[at\,\ell_1 \land \overline{y} = \overline{u} \land u_2 = 0 \land u_3 \cdot {u_1}^{u_2} = {x_1}^{x_2}]$
by $T24$ and PR

11. $\vdash \; [at\,\ell_1 \land u_2 = 0 \land \overline{y} = \overline{u}] \supset \Diamond[at\,\ell_2 \land \overline{y} = \overline{u}]$ by F'_β, $E2$, and PR

12.. $\vdash \; [at\,\ell_1 \land \overline{y} = \overline{u} \land u_2 = 0 \land u_3 \cdot {u_1}^{u_2} = {x_1}^{x_2}]$
$\supset \Diamond[at\,\ell_2 \land \overline{y} = \overline{u} \land u_2 = 0 \land u_3 \cdot {u_1}^{u_2} = {x_1}^{x_2}]$ by FR

13. $\vdash \; [u_2 = 0 \land u_3 \cdot {u_1}^{u_2} = {x_1}^{x_2}] \supset u_3 = {x_1}^{x_2}$ by domain

14. $\vdash \; [at\,\ell_2 \land u_2 = 0 \land u_3 \cdot {u_1}^{u_2} = {x_1}^{x_2}] \supset [at\,\ell_2 \land u_3 = {x_1}^{x_2}]$ by PR

15. $\vdash \; [at\,\ell_2 \land \overline{y} = \overline{u} \land u_2 = 0 \land u_3 \cdot {u_1}^{u_2} = {x_1}^{x_2}]$
$\supset [at\,\ell_2 \land y_3 = {x_1}^{x_2}]$ by $E2$ and PR

16. $\vdash\ Q(0,\overline{y}) \supset \Diamond\psi$ by 10, 12, 15 and $\exists\Diamond Q$

proof of (b_2): We have to consider three cases: $y_2 = 0$, $y_2 > 0 \wedge odd(y_2)$, and $y_2 > 0 \wedge even(y_2)$. Let us only prove the last case.

Case 3: $y_2 > 0 \wedge even(y_2)$.

17. $\vdash\ [Q(n+1,\overline{y}) \wedge y_2 > 0 \wedge even(y_2)] \supset [at\,\ell_1 \wedge \overline{y} = \overline{y}$
$\wedge\, y_2 > 0 \wedge even(y_2) \wedge (0 \le y_2 \le n+1) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}]$
by $E1$ and PR

18. $\vdash\ [Q(n+1),\overline{y}) \wedge y_2 > 0 \wedge even(y_2)] \supset \exists\overline{u}.[at\,\ell_1 \wedge \overline{y} = \overline{u}$
$\wedge\, u_2 > 0 \wedge even(u_2) \wedge (0 \le u_2 \le n+1) \wedge u_3 \cdot {u_1}^{u_2} = {x_1}^{x_2}]$
by $T24$ and PR

19. $\vdash\ [at\,\ell_1 \wedge \overline{y} = \overline{u} \wedge u_2 > 0 \wedge even(u_2)]$
$\supset \Diamond[at\,\ell_1 \wedge \overline{y} = ({u_1}^2,\ u_2 \div 2,\ u_3)]$ by F'_δ, $E2$, and PR

20. $\vdash\ [at\,\ell_1 \wedge \overline{y} = \overline{u} \wedge u_2 > 0 \wedge even(u_2)$
$\wedge\,(0 \le u_2 \le n+1) \wedge u_3 \cdot {u_1}^{u_2} = {x_1}^{x_2}]$
$\supset \Diamond[at\,\ell_1 \wedge \overline{y} = ({u_1}^2,\ u_2 \div 2,\ u_3) \wedge even(u_2)$
$\wedge\,(0 \le u_2 \le n+1) \wedge u_3 \cdot {u_1}^{u_2} = {x_1}^{x_2}]$
by FR

21. $\vdash\ [even(u_2) \wedge (0 \le u_2 \le n+1) \wedge u_3 \cdot {u_1}^{u_2} = {x_1}^{x_2}]$
$\supset [(0 \le u_2 \div 2 \le n) \wedge u_3 \cdot ({u_1}^2)^{u_2 \div 2} = {x_1}^{x_2}]$ by domain

22. $\vdash\ [at\,\ell_1 \wedge \overline{y} = ({u_1}^2,\ u_2 \div 2,\ u_3) \wedge even(u_2) \wedge (0 \le u_2 \le n+1)$
$\wedge\, u_3 \cdot {u_1}^{u_2} = {x_1}^{x_2}] \supset [at\,\ell_1 \wedge (0 \le y_2 \le n) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}]$
by $E2$ and PR

23. $\vdash\ [Q(n+1,\overline{y}) \wedge y_2 > 0 \wedge even(y_2)] \supset \Diamond Q(n,\overline{y})$
by 18, 20, 22, and $\exists\Diamond Q$

To summarize, we can show

$\vdash\ [Q(n+1,\overline{y}) \wedge y_2 = 0] \supset \Diamond\psi$ case 1

$\vdash\ [Q(n+1,\overline{y}) \wedge y_2 > 0 \wedge odd(y_2)] \supset \Diamond Q(n,\overline{y})$ case 2

$\vdash\ [Q(n+1,\overline{y}) \wedge y_2 > 0 \wedge even(y_2)] \supset \Diamond Q(n,\overline{y})$ case 3

Then since

$\vdash\ Q(n+1,\overline{y}) \supset [y_2 = 0 \vee (y_2 > 0 \wedge odd(y_2)) \wedge (y_2 > 0 \wedge even(y_2))]$ by domain

it follows that

$\vdash\ Q(n+1,\overline{y}) \supset [\Diamond\psi \vee \Diamond Q(n,\overline{y})]$ by PR

This concludes the alternative proof of the total correctness of our example. ∎

Acknowledgement

This exposition of temporal axiomatization and its application to the verification of deterministic, sequential programs emerged from work done in collaboration with Amir Pnueli on the temporal verification of concurrent programs. I wish to thank Amir for a most stimulating and enjoyable collaboration.

I am indebted to Jacques Hagelstein, Yoni Malachi, Ben Moszkowski, Pierre Wolper and Frank Yellin for their careful reading of the manuscript and for providing insightful comments. Special thanks are due to Evelyn Eldridge-Diaz for TEXing the manuscript.

REFERENCES

[BMP] Ben-Ari, M., Z. Manna and A. Pnueli, "The temporal logic of branching time," Proceedings of the Eighth ACM Symposium on Principles of Programming Languages, Williamsburg, VA, Jan. 1981, pp. 169-176.

[BUR] Burstall, R.M., "Program Proving as Hand Simulation with a Little Induction," Proc. IFIP Congress, Amsterdam, The Netherlands (1974), North Holland, pp. 308-312.

[GPSS] Gabbay D., A. Pnueli, S. Shelah, and J. Stavi, "The Temporal Analysis of Fairness," Proc. 7th POPL, Las Vegas, NV (January 1980), pp. 163-173.

[HC] Hughes, G.E. and M.J. Cresswell, *An Introduction to Modal Logic*, Methuen & Co., London, 1968.

[MP1] Manna, Z. and A. Pnueli, "Verification of concurrent programs: The temporal framework," in *The Correctness Problem in Computer Science* (R.S. Boyer and J S. Moore, eds.), International Lecture Series in Computer Science, Academic Press, London, 1981. Also, Computer Science Report, Stanford University, Stanford, CA (June 1981).

[MP2] Manna, Z. and A. Pnueli, "Verification of concurrent programs: temporal proof principles," Proc. of the Workshop on Logics of Programs (Yorktown-Heights, NY), Springer-Verlag Lecture Notes in Computer Science, 1981.

[MW] Manna, Z. and R. Waldinger, "Is 'Sometime' Sometimes Better Than 'Always'?: Intermittent Assertions in Proving Program Correctness," CACM, Vol. 21, No. 2, pp. 159-172 (February 1978), pp. 159-172.

[PNU] Pnueli, A., "The Temporal Logic of Program," Proc. 18th FOCS, Providence, RI (November 1977), pp. 46-57.

[PRI] Prior, A., *Past, Present and Future*, Oxford University Press, 1967.

[RU] Rescher and Urquhart, *Temporal Logic*, Springer Verlag, 1971.